uc3m | Universidad Carlos III de Madrid

Grado Universitario en Ingeniería de Sistemas de Comunicaciones
2017-2018

Trabajo Fin de Grado

Integración de recursos empresariales con la herramienta de "Acceso Remoto Unificado" (ARU)

Carmen María García Sánchez

Tutor

Julio Villena Román

Leganés, 2018

Este proyecto se lo quiero agradecer especialmente a mis padres, Joaquin y Josefa, que sin su apoyo incondicional no hubiera sido posible.
También quiero agradecer el apoyo y la paciencia de mi pareja Julio y de mis amigos. Sin ellos este camino no hubiera sido lo mismo.
Por último, agradecer a mi tutor Julio Villena por orientarme y guiarme en este trabajo. Sin su ayuda no lo habría conseguido.

RESUMEN

La herramienta ARU para el acceso remoto es una propuesta enfocada a las empresas para poder gestionar desde un mismo software los diferentes accesos, herramientas y recursos utilizados en el entorno laboral. Se unifican las configuraciones y se facilitan los accesos a los usuarios que, por cuestiones de viajes u horarios, tengan que teletrabajar.

El software que se va a utilizar para este trabajo es Pulse Secure. Veremos que abarca muchas funcionalidades entre las que se encuentra la integración con directorio activo, soporte para diferentes modos de autenticación y controlador de host entre otras integraciones. Con ello se va a demostrar que con una sola herramienta se puede gestionar toda una red corporativa, siendo el pilar más importante la seguridad a la hora de acceder a todos los recursos internos.

Para ello realizaremos diferentes casos prácticos en donde se expondrán distintos escenarios de empresas cuya necesidad les lleve a utilizar esta herramienta, pudiendo demostrar como Pulse Secure se integra con los recursos ya existentes en la red corporativa de la compañía.

Esta propuesta se ofrece a las empresas como una solución fácil, rápida y segura con la que poder trabajar cuando no se esté físicamente en la oficina. Con ello se optimiza el tiempo de trabajo además de los costes, pues sólo se necesitaría un servidor físico donde alojar la máquina virtual para la instalación del software. Así se evitaría un coste extra por la instalación de equipos adicionales.

Con ARU será como tener la oficina en casa, pudiendo acceder a la documentación que se encuentre en la intranet y sin la obligación de tener que instalar en el equipo personal software corporativo.

Palabras clave

ARU, Pulse Secure, VPN, Acceso Remoto Unificado, Teletrabajo, Directorio Activo, Host Checker.

EXTENDED ABSTRACT

Motivation

Teleworking, whether for business trips, holidays or meetings, is becoming more common. Taking into account that we are in a society that is in continuous movement, have begun to emerge numerous jobs that do not require going to the business center to develop their work.

As a first solution, employees have to take their equipment out of the office in order to have the information they have stored or record in an external storage device the information they consider necessary. However, this is not a viable or secure solution, because in addition to taking a device out of the business environment, there would be no access to internal tools or shared units, without forgetting that much of this documentation is protected because is confidential information.

This can be avoided thanks to tools that allow remote management of a computer located in the internal network of the office, facilitating access to users who are outside it and can work dynamically. But in some cases it takes more than one tool to complete the task, resulting in annoying. In addition, having to use different resources, can lead to vulnerabilities with the consequent risk to security.

For this reason it is important to be able to perform these functions in a secure manner, as there is a lot of confidential information and documents that requires it. A tool must be used to combine the security established in the company, together with the security of users who access from outside, without neglecting the fact that they need access to different business resources.

This is how the idea of this project appears, whose purpose is to present a tool that performs the tasks described above, unifying the remote access to other services, such as a terminal services or a web access, thus protecting and even encrypting the internal and confidential documentation.

We have called this tool ARU, for "Unified Remote Access". You can manage a whole network of portable and mobile devices as if you were directly connected to the internal network, providing from a single platform access to all the resources that are needed, customizing it according to the needs of each working group.

Target of project

The purpose of this Degree Project is to demonstrate that an integration of the different business resources can be carried out with a single tool that facilitates the unification of the different remote accesses, thus covering the needs of the companies. This is intended to unify the access to internal tools, as well as access to the documentation itself covering the potential gaps they have, such as the lack of security in their remote systems or the ability to perform tasks from anywhere in the world.

With the ARU tool, all the accesses, resources, documentation or programs of internal use will be unified in a single platform in a comfortable, fast and simple way, without having to use different applications to achieve the same result.

This results in greater labor productivity and better worker performance, because it provides access to the necessary resources and maintains the security established in the company from each of the configurations made with ARU.

Throughout this work will be studied the different processes and elements involved in the configuration to establish a fast and secure connection with the headquarters of a company. Getting employees of national and international companies to perform their day-to-day tasks without having to go to the office to do it.

The software that will be used for this work is Pulse Secure. We will see that it covers many functionalities among which is the integration with active directory, support for different authentication modes and host controller among other integrations. This will demonstrate that with a single tool you can manage an entire corporate network, being the most important pillar the security when you accessing all internal resources.

In order to demonstrate the scope of ARU, first discover the different elements that intervene in a business network and the uses that can be given. Second it will be detailed how ARU intervenes in these elements and finally there will be a section of practical cases, based on fictitious situations, but that could be real scenarios. In these scenarios, everything that has been seen throughout the project will be applied and the different configurations will be made to enable both remote access and the different resources of a company.

Regulatory framework

To carry out this project, we must keep in mind that the privacy and security of correctly safeguarding all information related to a company is of vital importance, since it is a project whose purpose is to teach the different combinations that can be made to unify the tasks and resources of a company, you will have access to all kinds of confidential information, and therefore, you have to guarantee that you will not access those unauthorized personal resources. To this effect, internal servers owned by the company, active directories and antivirus deployed on all computers will be used.

Of course, the company must take care that all the licenses of the tools to be used are valid and are in force, since they are payment tools that are usually hired by cycles.

Additionally, if this solution is implemented in a company, this tool must adapt to the standards applied in that company, such as the fact of complying with an ISO (International Standardization Organization) such as ISO 20,000 among others.

Also take into account, although not directly applicable to this project, the application used is based on the IEEE (Institute of Electrical and Electronics Engineers) standards, such as IEEE 802.11.

Finally, it is very important to comply with the data protection law. If this project is carried out in a company, it must comply with the new European regulation GDPR (General Data Protection Regulation) that came into force in May 2018. With this regulation, the data of all the users who are both on the platform of ARU as in the company itself should be confidential and for internal use.

Abstract

ARU remote access tool is a proposal focused on companies to manage the different accesses, tools and resources used in the work environment from the same software. The configurations are unified and access is provided to users who, due to travel or schedules, have to telecommute.

The software that will be used for this work is Pulse Secure. We will see that it covers many functionalities like integration with active directory, support for different authentication modes and host controller among other integrations. This will demonstrate that with a single tool you can manage an entire corporate network, being the most important pillar the security when you accessing all internal resources.

In order to do this we will make different case where different scenarios of companies whose need will lead them to use this tool will be exposed, being able to demonstrate how Pulse Secure integrates with existing resources in the corporate network of the company.

With this proposal, the company is offered an easy, fast and safe solution with which to work when not physically in the office. This optimizes the working time in addition to the costs, since only a physical server would be needed to host the virtual machine for the software installation. This would avoid an extra cost for the installation of additional equipment.

This proposal is offered to companies as an easy, fast and safe solution with to work when they are not physically in the office. This optimizes the working time in addition to the costs, considering that they only need a physical server to host the virtual machine for the software installation. This would avoid an extra cost for the installation of additional equipment.

With ARU it will be like having the office at home, being able to access the documentation that is on the intranet and without the obligation of having to install corporate software on the personal computer.

Pulse Secure based solution

To carry out the objectives of this work, we are going to use a unique tool that unifies all the services already implemented by the company. This tool is Pulse Secure software.

This software offers several functionalities that can be applied to a company's environment. These options are focused, among other things, on:

- Types of authentication: They can be local, Active Directory, LDAP or SAML.

- Access modes: VPN, SSH, HTTP.

- Security protocols: SSL / TLS, IPsec.

With Pulse Secure you can, for example, carry out an integration in the directory, as users who can access the different resources that have permissions, such as the mail of the company, with the previous step to fulfill the requirements of security by the company. These requirements can be the same from where you have access to antivirus with the test correctly and have the operating system in Windows 7.

Regarding security, Pulse Secure has the Host Checker tool that analyzes the computer with the established policies and in case of non-compliance, access to the intranet will not be allowed. This ensures that the internal security of the company is not transferred, avoiding possible malware. It can also be combined with more complex integrations such as the double authentication factor.

Conclusions

Once the description and use of the ARU tool to integrate various business resources has been completed, it has been demonstrated that this proposal is easily adapted to business uses, without focusing on enhancing a resource, such as remote access. This offers the company the opportunity to obtain, according to their needs and existing configurations in their network, a complete, safe and user-friendly platform.

As we have seen throughout this project, security has been given considerable importance to different resources and different ways of implementation and combination have been demonstrated. An example can be an integration whose security applied to the users with a double factor of authentication together with the requirement of host checker applied to the device of said user.

After demonstrating the use and realization of integrations with different levels of complexity, it can be affirmed that ARU adapts to all types of companies and has an important flexibility of the service, being able to integrate from an LDAP directory to simply local users. Therefore, it can finally be concluded that the objectives set in this project have been met and that the results obtained have been positive.

Future works

The needs to be able to access your business resources outside the office are becoming more common, as workers take advantage of the journey of work trips to go ahead what they have to do in the destination and finalize the details of their meetings, or they need to connect at dawn if there has been any alarm in the services managed by the companies.

Therefore, not only depends on a computer, but now they have smartphones or tablets where they can perform that same work. Sometimes, it is more convenient to use the mobile device and not have to carry a computer in case it is needed.

So as future work is proposed to use the same solution provided for computers, but for mobile devices and tablets. That is, use Pulse Secure applied to Smartphones and tablets. Being a software compatible with Android, iOS and Windows Phone, the scope for the implementation of this solution is very broad.

It would be necessary to perform tests in different environments to study their behavior, in addition to checking the configurations offered in each operating system, as they do not have to support the same functions, since they are based on different operating systems.

This will improve the user's communication with the office, achieving greater convenience at the time of having to perform certain procedures or access to internal documentation, and improve the speed of access where Smartphone or Tablet is usually powered on and you do not need to have a place to work. With this, an extra is obtained as a complement to the solution provided for computers.

With this new proposal, a complete service will be obtained and it will cover all the operative systems and will facilitate the work to the users. Being able to achieve an improvement in productivity and minimize the problems that can be caused by not having a tool that facilitates and manages the access to the different necessary resources.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

INDICE DE TABLAS

1. INTRODUCCIÓN

1.1 Motivación

El teletrabajar, ya sea por motivos de viaje de negocios, vacaciones o reuniones, es cada vez más habitual. Teniendo en cuenta que nos encontramos en una sociedad que está en continuo movimiento, han empezado a surgir numerosos trabajos que no requieren acudir al centro empresarial para poder desarrollar su labor.

Como primera solución, los empleados tienen que sacar su equipo de la oficina para poder disponer de la información que tienen almacenada o grabar en un dispositivo de almacenamiento externo la información que consideren necesaria. Sin embargo, esto no es una solución ni viable ni segura, ya que además de sacar un dispositivo fuera del entorno empresarial, no se tendría acceso a las herramientas internas o unidades compartidas, sin olvidar que mucha de esa documentación está protegida al tratarse de información confidencial.

Esto se puede evitar gracias a herramientas que permiten la gestión remota de un equipo situado en la red interna de la oficina, facilitando los accesos a los usuarios que se encuentren fuera de ésta y pudiendo trabajar de forma dinámica. Pero en algunos casos hace falta más de una herramienta para poder completar dicha tarea, resultando tedioso realizar el trabajo correspondiente. Además, al tener que utilizar diferentes recursos, puede acarrear vulnerabilidades con el consiguiente riesgo en la seguridad.

Por esta razón es importante poder realizar dichas funciones de forma segura, pues hay muchos datos e información confidencial que lo requieren. Se debe utilizar una herramienta que permita combinar la seguridad establecida en la empresa, junto con la seguridad de los usuarios que acceden desde fuera, sin dejar de lado el hecho de que necesitan acceso a diferentes recursos empresariales.

Así nace la idea de este proyecto, cuya finalidad es presentar una herramienta que realice las tareas anteriormente descritas, unificando el acceso remoto a otros servicios, como puede ser un *terminal services* o un acceso web, así protegiendo e incluso cifrando la documentación interna y confidencial. A esta herramienta la hemos denominado ARU, por “Acceso Remoto Unificado”. Con ello se podrá gestionar toda una red de dispositivos portátiles y móviles como si estuvieras conectado directamente a la red interna, proporcionando desde una única plataforma el acceso a todos los recursos que se necesiten, personalizándolo según las necesidades de cada grupo de trabajo.

1.2 Objetivos

Este Trabajo Fin de Grado tiene como objetivo demostrar que se puede realizar una integración de los diferentes recursos empresariales con una única herramienta que facilite la unificación de los diferentes accesos remotos, cubriendo así las necesidades de las empresas. Con ello se pretende unificar los accesos a las herramientas internas, así como el acceso a la documentación propia cubriendo las posibles carencias que tengan, como puede ser la falta de seguridad en sus sistemas remotos o la posibilidad de poder realizar tareas desde cualquier parte del mundo. Con la herramienta ARU, se unificarán en una sola plataforma todos los accesos, recursos, documentación o programas de uso interno de forma cómoda, rápida y sencilla, sin necesidad de tener que utilizar aplicaciones diferentes para conseguir el mismo resultado.

Con esto se consigue mayor productividad laboral y mejor rendimiento del trabajador, porque se le facilita el acceso a los recursos necesarios y se conserva la seguridad establecida en la empresa desde cada una de las configuraciones realizadas con ARU.

A lo largo de este trabajo se estudiarán los diferentes procesos y elementos que intervienen en la configuración para poder establecer una conexión rápida y segura con la sede de una empresa. Consiguiendo que los empleados de empresas nacionales e internacionales puedan realizar sus tareas del día a día sin tener que ir a la oficina para realizarlo.

El software que se va a utilizar para este trabajo es Pulse Secure. Veremos que abarca muchas funcionalidades entre las que se encuentra la integración con directorio activo, soporte para diferentes modos de autenticación y controlador de host entre otras integraciones. Con ello se va a demostrar que con una sola herramienta se puede gestionar toda una red corporativa, siendo el pilar más importante la seguridad a la hora de acceder a todos los recursos internos.

Para poder demostrar el alcance que tiene ARU, primero se descubrirán los diferentes elementos que intervienen en una red empresarial y los usos que se le pueden dar. Segundo se detallará cómo interviene ARU en esos elementos y finalmente habrá un apartado de casos prácticos, basados en situaciones ficticias, pero que podrían tratarse de escenarios reales. En estos escenarios se aplicará todo lo que se ha visto a lo largo del proyecto y se realizarán las diferentes configuraciones para habilitar tanto accesos remotos como a los diferentes recursos de una empresa.

1.3 Marco regulador

Para llevar a cabo este proyecto, debemos tener presente que la privacidad y la seguridad de salvaguardar correctamente toda información relativa a una empresa es de vital importancia, ya que al tratarse de un proyecto cuya finalidad es enseñar las diferentes combinaciones que se pueden realizar para unificar las tareas y recursos de una empresa, se tendrá acceso a toda clase de información confidencial, y por tanto, hay que garantizar que no accederán a esos recursos personal no autorizado. Para ello se utilizarán servidores internos propiedad de la empresa, directorios activos y antivirus desplegado en todos los equipos.[1]

[1] https://www.powerdata.es/seguridad-de-datos

Por supuesto, la empresa debe hacerse cargo de que todas las licencias de las herramientas a utilizar sean válidas y estén vigentes, pues son herramientas de pago que se suelen contratar por ciclos.

Adicionalmente, si se implanta esta solución en una empresa, dicha herramienta deberá adaptarse a los estándares que se apliquen en esa compañía, como puede ser el hecho de cumplir una ISO (*Organismo Internacional de Estandarización*) como la ISO 20.000 entre otras. [1]

También tener en cuenta, aunque no aplique directamente a este proyecto, la aplicación utilizada se basa en los estándares IEEE (*Institute of Electrical and Electronics Engineers*), como por ejemplo, en el IEEE 802.11. [2]

Por último, es muy importante que se cumpla la ley de protección de datos. Si se lleva a cabo este proyecto en una empresa está deberá atenerse al nuevo reglamento europeo GDPR (*General Data Protection Regulation*) [2] que entró en vigor en mayo del 2018. Con este reglamento, los datos de todos los usuarios que se encuentren tanto en la plataforma de ARU como en la propia empresa deberán ser confidenciales y de uso interno. [3]

[2] https://www.eugdpr.org/

2. ESTADO DEL ARTE

En un entorno empresarial existen integraciones, como puede ser un directorio activo, que están configuradas dentro de la red y que facilitan los accesos a documentación, así como a herramientas internas, evitando que un usuario pueda utilizar un recurso para el que no tiene permiso.

A la hora de realizar una gestión remota, hay que tener en cuenta estos mismos criterios. Se deben cumplir las mismas directrices que están establecidas dentro del entorno laboral, y por ello, es necesario conocer los elementos que intervienen en la red y cómo están configurados.

Por este motivo, se van a describir las configuraciones más características y utilizadas en el entorno de una red empresarial. Se explicarán los métodos de acceso que existen para conectarse a una red en remoto, así como los modos que hay para autenticarse a dicha red desde casa, sin olvidar la seguridad necesaria para establecer la conexión con el equipo que se encuentra en la oficina.

2.1 Modos de autenticación

A la hora de establecer una conexión mediante un túnel, no es simplemente escribir nombre de usuario/contraseña y realizar comunicación con el otro extremo, sino que requiere de algo más. Requiere de unos pasos intermedios, los cuales brindan la seguridad necesaria a la conexión, para que a la hora de enlazar los permisos, el túnel no sea vulnerable.

Uno de estos pasos es la autenticación del usuario. Es decir, que la persona que está tratando de acceder a dicha conexión es quien dice ser y se le dará permiso para acceder a una aplicación, plataforma o servicio, siempre y cuando tenga autorización para utilizar esos recursos. Para autenticar al usuario existen diversos modos, pero en este proyecto veremos cuatro de ellos, que serán Locales, Directorio Activo, LDAP y 2FA.

No obstante, esto no quita que se pueda franquear dicha seguridad y accedan al sistema terceras personas, pero será complicado de lograr, y desde luego, llevará tiempo realizarlo. Es por ello, que es altamente recomendable cambiar la contraseña del usuario cada ‘X’ días/meses.

Para comenzar a explicar los diferentes tipos de autenticación se va a empezar por el más básico, sencillo, y por tanto, más vulnerable y menos seguro, hasta el más avanzado, complejo, y por tanto, seguro.

2.1.1 Autenticación local

La autenticación de usuarios locales es la más básica, pues no requiere de instalaciones complejas previas.

Esta autenticación funciona de la siguiente manera: A un usuario se le crea un nombre y contraseña, siendo estos datos los que deberá introducir cuando desee acceder al túnel que establece la conexión con los recursos a los que quiere acceder, ya sea su oficina o herramientas privadas cómo el correo electrónico, entre otros.

Tal y como se muestra en las figuras 2.1.1 y 2.1.2, estos usuarios se encuentran almacenados en una base de datos asociada a la herramienta (recurso) que se va a utilizar. Consta de un nombre y una contraseña, la cual se tendrá que escribir cada vez que el usuario particular quiera abrir un túnel (Fig.2.1.2) o acceder al recurso en cuestión (Bookmark, *terminal Service*, Correo corporativo…) como en la Fig.2.1.1.

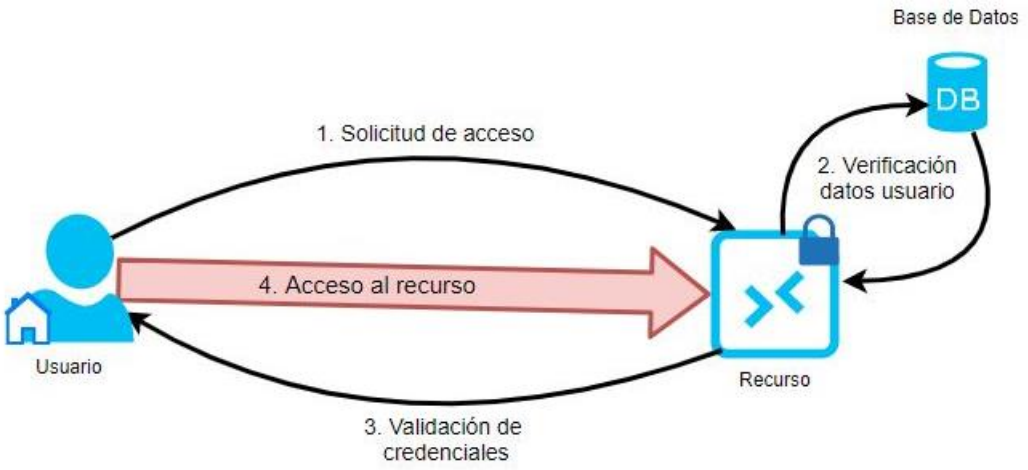

Fig. 2.1.1: Autenticación local con acceso a un recurso

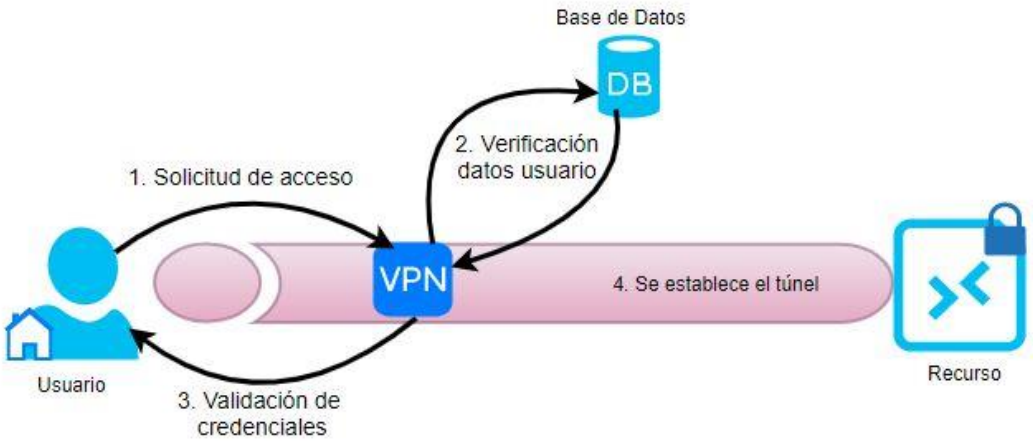

Fig. 2.1.2: Autenticación local a través de un túnel

Cómo es de imaginar, este sistema de autenticación no es muy seguro, pues cualquier persona con acceso a la base de datos puede alterar los datos e incluso suplantar al usuario. Además, al ser una contraseña que sólo se encuentra en ese archivo, se podría cambiar fácilmente con el simple hecho de, por ejemplo, acceder a "¿Has olvidado la contraseña?" y modificarlo.

A pesar de todo ello es un método bastante utilizado porque no requiere integraciones extras, basta con crear usuario y contraseña. El inconveniente es que es la opción menos segura, pues no validas contra nada más y las empresas pueden correr el riesgo de que entren en sus sistemas internos. Esto es algo que no se tiene en cuenta debido a la poca conciencia que hay sobre la vulnerabilidad en la red y la seguridad en la misma.

2.1.2 Autenticación con directorio activo

El Directorio Activo (DA) es un servicio de directorio en donde se almacenan todos y cada uno de los usuarios que pertenecen a esa empresa, además de los respectivos equipos. Cada uno de estos elementos se conoce como objetos de un directorio y este tiene el objetivo de administrar tanto las políticas de red como los accesos a los equipos conectados a la misma. Toda esta información se encuentra almacenada en una base de datos de la compañía a la cual se puede acceder desde diferentes servicios para garantizar la seguridad y correcto funcionamiento de todos los recursos implicados [4].

En este directorio se encuentran descritas las jerarquías de los diferentes grupos existentes en la compañía. Además, cada usuario se encuentra asociado a uno o varios grupos, los cuales tendrán ciertos permisos y/o privilegios, pudiendo diferir entre ellos para facilitar el acceso a los diferentes recursos.

Una estructura de Directorio Activo está compuesta por los siguientes elementos [4]:

- Unidad Organizativa (OU (*Organizational Unit*)): Es el elemento más básico de esta estructura. Está compuesto por diferentes elementos, como pueden ser impresoras, usuarios, grupos…

- Dominio: Es un conjunto de objetos que forman una unidad administrativa. Para poder comunicar los diferentes dominios se establecen relaciones de confianza creadas automáticamente cada vez que se añade un nuevo dominio.

- Árbol de directorio: Abarca todos los dominios que se encuentran en una empresa ordenados jerárquicamente. Con todos los elementos anteriores se construye el árbol de directorio.

- Bosque: Es el conjunto de todos los árboles de directorio que tenga una entidad. Cómo mínimo tiene que tener un árbol de directorio, el cuál será del dominio raíz y contendrá todos los dominios anteriores.

A modo de ejemplo, en la figura 2.1.3 se observa una estructura de AD de una empresa formada por diferentes dominios y unidades organizativas, las cuales forman parte de un árbol de directorio, que a su vez pertenece a un bosque.

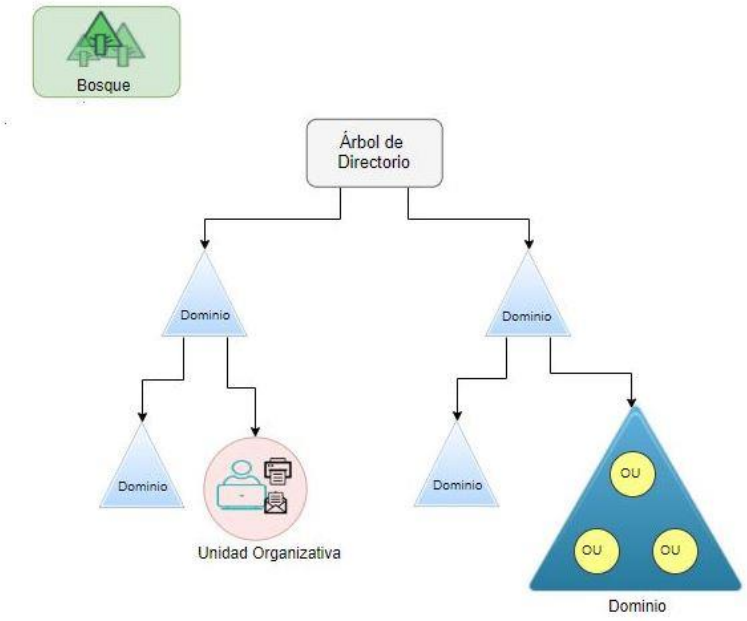

Fig. 2.1.3: Estructura de Directorio Activo

En el caso de un servicio de directorio de Windows Server, se puede distinguir un esquema similar al de la figura 2.1.4, en donde tendríamos un solo árbol de directorio, compuesto por un directorio raíz, llamado *contoso.com*, formado por un DC=contoso y DC=com. Este, a su vez, incluye diferentes dominios como pueden ser *Atlántico* formado por OU=Atlántico. [5]

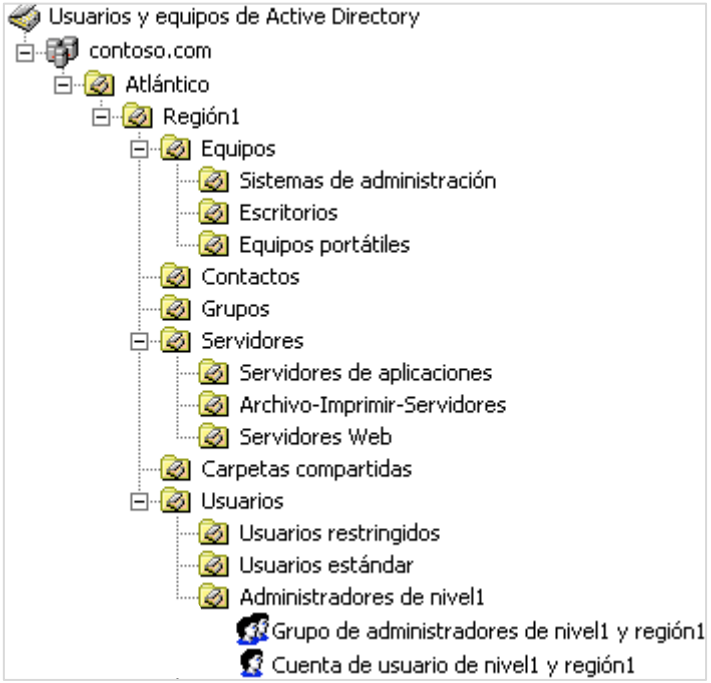

Fig. 2.1.4: DA Windows Server **[5]**

En la siguiente figura se puede ver el esquema genérico de una autenticación con directorio activo, en la que tras solicitar el acceso, se introducen las credenciales de usuario las cuales son autenticadas por el directorio y, si este tiene permiso de acceso al recurso solicitado, podrá acceder correctamente al mismo.

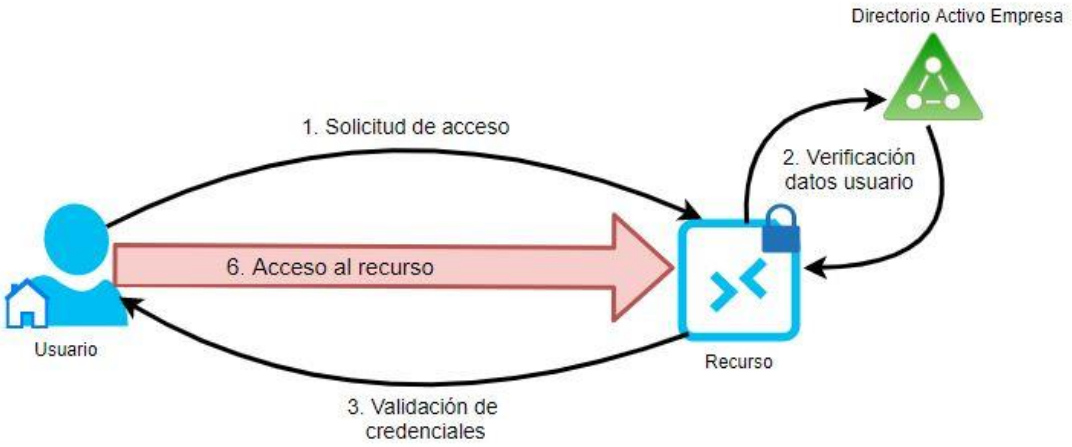

Fig. 2.1.5: Esquema de autenticación por DA

Este proceso se lleva a cabo mediante una conexión TLS/SSL sobre un DC (*Domain Controller*). Durante el establecimiento de comunicación, el DC solicita el certificado de cliente y si este es válido servirá para la autenticación de la conexión, cuyas credenciales serán las aportadas por ese certificado. Una vez establecida la comunicación el Access Point, utilizando las credenciales de administrador del DA, se enlaza con el DC. En caso de que este enlace sea validado, el AP buscará los datos del usuario según el atributo correspondiente y si lo encuentra se devolverá el Distinguished Name del usuario. Para finalizar, se probará a enlazar el AP con los datos introducidos previamente y si estas credenciales son válidas se autenticará el usuario.

Por otro lado, a diferencia del DA que está basado en Microsoft Windows Server, LDAP (Lightweight Directory Access Protocol) es un protocolo que permite el acceso a diferentes servicios de directorio de una empresa, pero fundamentado sobre entornos Linux/Unix e implementado con soluciones basadas en código abierto. La estructura de este protocolo también es jerárquica en modo árbol y almacena, entre otras cosas, la información de usuarios como puede ser nombre, contraseña, correo, certificados, grupos, teléfono, permisos… Pudiendo hacer uso de estos atributos para determinar si el usuario que se está intentado logar para acceder a un recurso es o no válido. [6]

Por tanto, ambos servicios de directorio son válidos, únicamente dependerá de la estructura que se tenga y de lo que se quiera realizar, pues cada uno tiene sus limitaciones.

Aunque a priori parece algo sencillo de utilizar, se precisa de unos pasos previos para que desde la plataforma se pueda acceder a los datos de la empresa y se establezca un vínculo de confianza mutua. Para llevarlo a cabo se tiene que estudiar la configuración que tiene la empresa y trasladarlo a la plataforma habilitando las comunicaciones y los permisos para poder leer su DA/LDAP.

Aplicando todo lo anterior a nuestro servicio ARU, vemos que esas funcionalidades le dan valor a la autenticación con Directorio Activo o LDAP, pues sólo con logarse con las credenciales particulares del usuario ya se conoce los accesos o recursos a los que tiene permitido entrar.

Todo esto contribuye a la seguridad y a la administración de los accesos a los diferentes recursos que se realizan en el entorno de la empresa, pudiendo obtener información sobre quien, cuando y de cuánto tiempo ha sido la conexión de cada usuario, entre otras cosas.

2.1.3 Doble factor de autenticación (2FA)

Hoy en día es muy importante tener cuidado desde donde accedemos a nuestras cuentas personales y que tipo de contraseñas utilizamos. Es por ello que este último modo de autenticación es el más complejo y seguro de los modos descritos. Se trata de 2FA (*Two Factor Authentication*), que consiste en habilitar dos factores de autenticación para aumentar la seguridad de acceso a cualquier recurso de la empresa.

En este caso no bastará con que el usuario se autentique y dichas credenciales se validen, sino que además deberá pasar otro nivel más de seguridad. Una vez superado la primera autenticación, se solicitará una segunda y si dicha respuesta no es correcta, se denegará el acceso al recurso requerido por el usuario.

Este método se basa en realizar una combinación de dos de las siguientes opciones: Solicitar al usuario algo que él sabe, algo que tiene y/o alguna característica biométrica. Con esto se consigue que las probabilidades de usurpación de identidad disminuyan, pues dicha persona/máquina deberá tener dos de las tres opciones que pertenecen al usuario. [7] [8]

Como cabe esperar, las combinaciones que se pueden realizar son muy diversas, como por ejemplo, pedir unas credenciales de acceso y una tarjeta de crédito de la misma persona o la solicitud al usuario de sus credenciales e introducir un código que se le mandará a su teléfono móvil. Sólo si se superan ambas pruebas se podrá acceder al recurso solicitado.

A modo de ejemplo, tenemos otra opción más compleja, que consiste en la solicitud de las credenciales de directorio activo y la solicitud de su DNI a través de un lector de DNIe. Como se observa en la figura 2.1.6, primero se solicitan las credenciales de DA, en caso de que fueran incorrectas, se devuelve un aviso al usuario indicando que el acceso ha sido denegado. Si por el contrario estas son correctas, se validan y se procede a solicitar el DNI. Una vez se comprueba que el DNI introducido se corresponde con el atributo del DNI del usuario de directorio, este podrá acceder al recurso seleccionado. En cualquier otro caso, se denegará el acceso. [9]

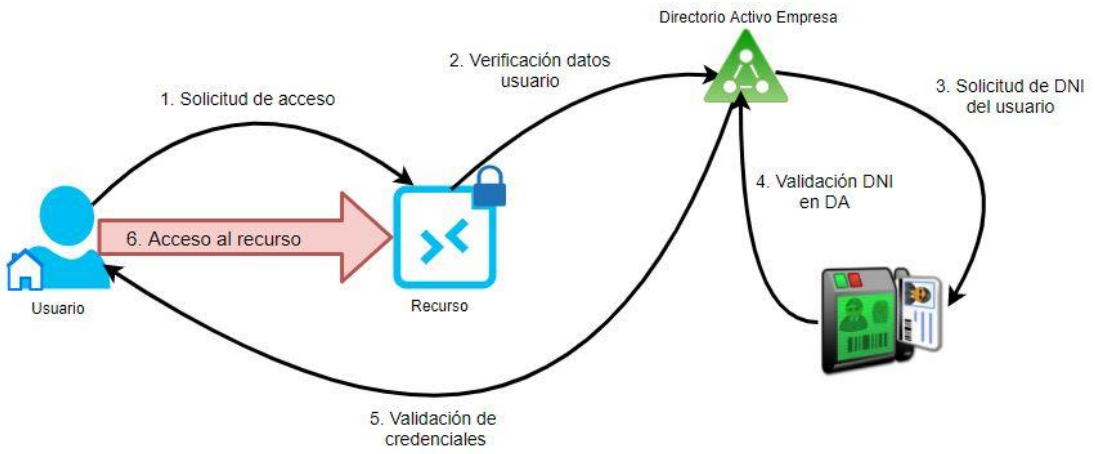

Fig. 2.1.6: Esquema de autenticación por 2FA con DNIe

Como se ha podido observar, con este método de autenticación si no se cumplen los dos requisitos no se podrá validar la autenticación, y por tanto, se denegará el acceso al recurso deseado.

Este tipo de autenticación evita tener que aprenderte las respuestas a las preguntas de seguridad, o a recordar un pin y además suelen tener un tiempo de expiración, por ejemplo si se genera una clave aleatoria, o el tiempo entre una autenticación y la siguiente es demasiado.

2.2 Modos de acceso

Todos los accesos de control remoto parten de la idea de permitir al usuario final realizar cualquier tipo de acción que requiera una comunicación con otra infraestructura. Siendo esta de la forma más sencilla/básica posible, pues el usuario no tiene por qué tener conocimientos del funcionamiento (interno) de esta clase de accesos. A su vez, el manejo de la herramienta que permita realizar dichas comunicaciones debe ser sencillo.

Hoy en día existen diferentes tipos de accesos para con un mismo fin. Dependiendo cómo se apliquen y con qué otras herramientas se combinen, el resultado que se obtiene puede ser completamente diferente.

A continuación estudiaremos tres modos de acceso: VPN, Túnel SSH y HTTP

2.2.1 Acceso VPN

La red VPN (*Virtual Private Network*) está diseñada para garantizar un acceso seguro a una red privada a través de una red pública. Esto consiste, a grandes rasgos, en la implementación o creación de un túnel que tiene como objetivo establecer una comunicación rápida y segura con recursos que se encuentran físicamente fuera del alcance de donde estás ahora. Hay que tener presente que para realizar esta comunicación, previamente el usuario en cuestión se ha tenido que autenticar y posteriormente se ha comprobado que dicho usuario tiene permiso para acceder al recurso solicitado, y por tanto, se valida su usuario y contraseña. Una vez que se ha logado correctamente, se levanta el túnel de VPN, y la información que viaja a través del mismo será cifrada con el método elegido para ello (más adelante hablaremos de los protocolos de seguridad que se pueden implementar con esta tecnología). [10]

A la hora de establecer el túnel de VPN hay que tener en cuenta también que, en el otro extremo al que queremos acceder, debe estar permitido nuestro acceso y vigilar que el Firewall no nos bloquee la conexión.

Para ello, hay que revisar los permisos del firewall y comprobar que están abiertos los rangos de IP que proporciona la conexión VPN. En caso de que no estén permitidos habría que modificarlos para que se permita este acceso de VPN en concreto.

En la siguiente figura se observa un esquema básico de una conexión en remoto estableciendo un túnel VPN. El usuario en remoto (VPN Client) establece una conexión vía tunel con el servidor que dará acceso a la red interna de la empresa. Previamente se han habilitado los puertos

necesarios para que el firewall no bloquee el acceso y así acceder al ordenador del usuario en la oficina. [10] [11]

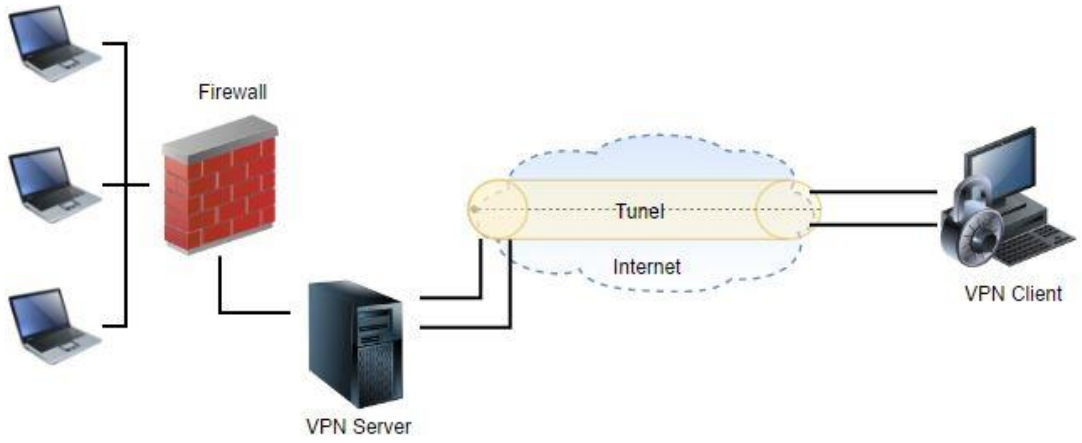

Fig. 2.2.1: Esquema básico de una red VPN

Esta tecnología es una de las más usadas hoy en día debido a su bajo coste, ya que no hace falta tener desplegada una costosa arquitectura para que un usuario pueda acceder a sus documentos a pesar de encontrarse en otro punto geográfico, su fácil mantenimiento, porque no necesita servicios extras ni aumentar o modificar la infraestructura existente en la empresa, además de fomentar el teletrabajo y reducir costes.

Además uno de los puntos fuertes es la seguridad que garantiza en la medida de lo posible, tanto al usuario como a la propia empresa, que el acceso a documentos internos no se vaya a filtrar o extraviar por la red. Es por eso que los documentos se cifran cuando se acceden mediante una conexión de VPN, con previa confirmación sobre la autenticación del usuario que está solicitando el acceso. [De este tema en particular hablaremos más adelante, ya que va de la mano de la herramienta aquí expuesta.]

Como veremos más adelante, la red VPN permite dar al usuario acceso remoto a las herramientas corporativas, tal y como muestra la figura 2.2.2. Estos accesos se pueden realizar de diferentes formas según esté montada la infraestructura de la empresa y según sea la finalidad de la misma. [10]

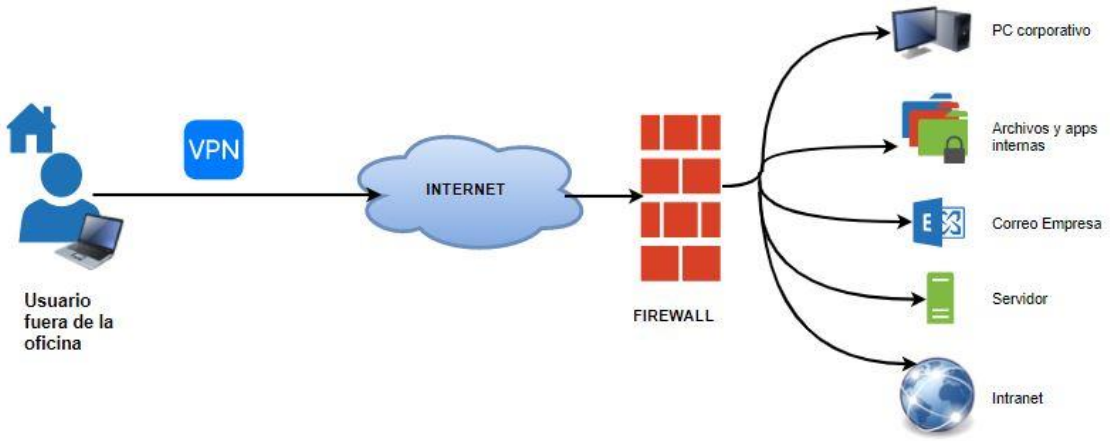

Fig. 2.2.2: Ejemplos de acceso interno a través de una VPN

En nuestro caso, el tipo de conexión que se va a utilizar estará basado en un Software denominado Pulse Secure.

Resumiendo, las ventajas que se obtienen por la utilización de redes VPNs son [12] [13]:

- Rápido acceso a recursos que se encuentran en diferentes puntos geográficos.
- Seguridad en el manejo de datos, ya que todo lo que va a través de la red VPN se cifra/encripta. Además de evitar que otras personas ajenas a la conexión establecida puedan acceder u obtener información interna o confidencial.
- Reducción del coste debido a que no se necesita una infraestructura nueva o adicional para su utilización.
- Fácil manejo.

Por otro lado, una de las desventajas que se puede encontrar va directamente relacionada con el dispositivo que se encuentra en el otro extremo de la conexión, puesto que si este tiene alguna brecha en la seguridad, se verá directamente afectado el enlace, y por tanto, el dispositivo origen. También puede repercutir en la velocidad de acceso que se experimenta tras incluir un mayor número de capas de cifrado y seguridad poniendo en riesgo la estabilidad de la conexión. Ambas opciones son mejorables con esta herramienta. [12] [13]

2.2.2 Acceso Túnel SSH + HTTP

En este caso nos encontramos con dos protocolos cuya combinación resulta ser de gran utilidad, y por tanto un gran aporte para el uso seguro de este servicio.

Por un lado, está SSH (Secure SHell) cuyo protocolo es más sencillo, vulnerable y limitado (a dos conexiones) respecto al túnel VPN. Estas características no permiten ciertas configuraciones que necesitan las empresas, por ello este va más enfocado a nivel de usuario y VPN a un nivel de escala superior. [14] [15]

Se suele emplear para administrar sistemas remotamente o navegar/transferir archivos desviando el tráfico, siempre cifrado, a otro equipo para evitar su intercepción. Al estar restringido a dos máquinas, el túnel se utiliza para una única aplicación y de ahí su limitación.

En la siguiente figura vemos un ejemplo de un recurso intentando acceder al Servidor remoto sin éxito por la presencia del firewall. Es por ello que se establece el túnel SSH permitiendo la comunicación entre cliente y servidor.

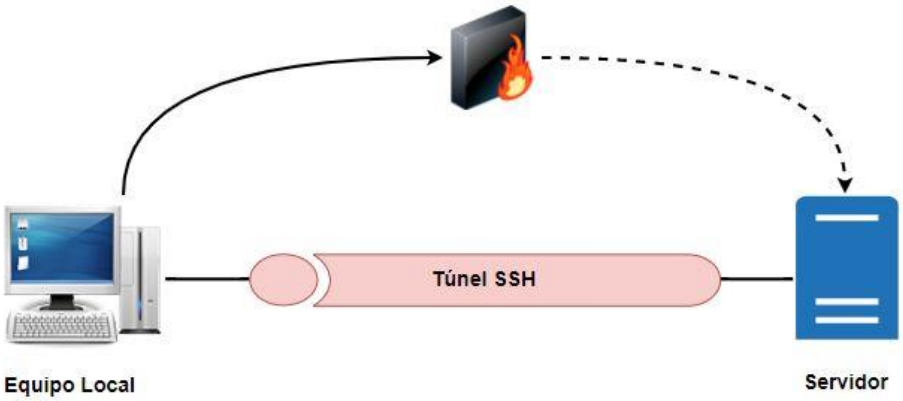

Fig. 2.2.3: Acceso a través del túnel SSH

Por otro lado, está el protocolo HTTP (Hypertext Transfer Protocol) que está basado en una estructura cliente-servidor cuyas comunicaciones se basan en TCP/IP y su principal función es transmitir información entre ambos dando lugar a lo que hoy en día se conoce como Internet. Este tipo de acceso se puede utilizar cuando la conexión se realiza a través de un Proxy Server o Firewalls, bloqueando el acceso y el tráfico que se inicia fuera de nuestra red, y a su vez enmascarando la dirección IP de origen para aumentar la seguridad al establecer el túnel de acceso a la intranet de la empresa. [16] [17]

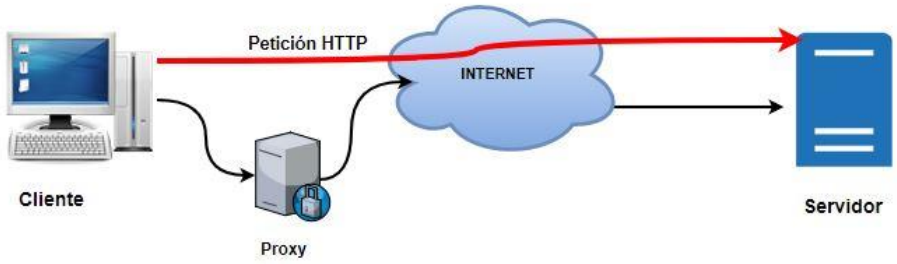

Fig. 2.2.4: Protocolo HTTP

Es por ello, que al combinar ambos accesos obtenemos una conexión segura y cifrada, además de poder acceder al exterior atravesando el bloqueo del proxy/firewall gracias al protocolo SSH. [18]

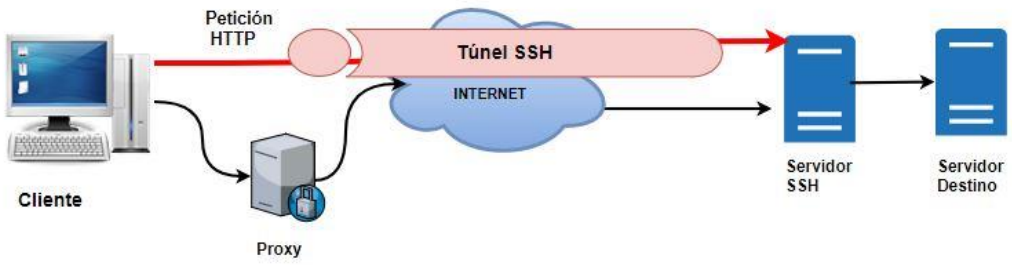

Fig. 2.2.5: Túnel SSH + HTTP

En relación a este proyecto y basándonos en lo expuesto anteriormente, nos vamos a centrar en el acceso VPN con el cual se van a realizar accesos a diferentes recursos (Bookmarks o *Terminal Services*) como veremos más adelante.

2.3 Protocolos de seguridad

Una parte importante a tener en cuenta cuando hablamos de realizar acciones en remoto, sobre todo si se trata de acceder a documentación e información de una empresa, es la seguridad en intercambiar datos por la red estableciendo una conexión segura y fiable que nos garantice que durante esa sesión nuestros datos estarán protegidos.

De modo que a través de los protocolos de seguridad establecidos en el momento de la conexión, el intercambio de datos será encriptado y así se podrá evitar que un posible ataque de un tercero nos robe la información o aparezcan agujeros de seguridad.

Para comprender mejor su comportamiento se va a explicar algunos de los protocolos de seguridad más utilizados y los cuales se aplican en nuestra herramienta.

2.3.1 SSL/TLS

El protocolo más conocido y utilizado es SSL/TLS (*Secure Sockets Layer/Transport Layer Security*). Esta tecnología se encarga de securizar nuestra conexión protegiendo la información que se transporte a través de la misma evitando que sea interceptada por terceros y se produzcan posibles robos de datos personales, bancarios, internos de una empresa, etc. [19]

Los principales objetivos de SSL se agrupan en tres conceptos importantes: [19]

- Autenticación: El protocolo SSL permite el uso de técnicas criptográficas de cifrado de clave pública para autenticar al cliente y servidor que establecen la comunicación.
- Integridad: Se garantiza la integridad de los datos durante la sesión para que no se puedan manipular de forma involuntaria o intencionada.
- Protección: La privacidad de los datos es algo bastante delicado, es por eso que los datos en el transporte entre cliente y servidor deben ser legibles solo por el destinatario y estar protegidos de una posible intercepción.
  Esto se aplica tanto al tráfico durante las negociaciones como a los datos de la aplicación que se envían durante la sesión:
  - SSL Record Protocol → Garantiza la seguridad e integridad de los datos.
  - SSL Handshake Protocol, SSL ChangeCipher SpecProtocol, SSL Alert Protocol → Establecen la conexión SSL.

SSL/TLS se encarga de proporcionarnos un enlace seguro y encriptado entre dos máquinas o entre dos elementos conectados a internet, como puede ser el acceso a una web a través de un navegador en cuyo caso se observará que en la url aparecerá HTTPS (*HyperText Transfer Protocol Secure*) en lugar de HTTP (*HyperText Transfer Protocol*). Este es el uso más común y extendido, pero gracias a que la capa de SSL Record Protocol se encuentra debajo de la capa de protocolos de aplicaciones y encima del protocolo TCP, este permite trabajar de forma transparente con los protocolos que utilizan TCP (*Transmission Control Protocol*) ofreciendo seguridad a las aplicaciones. [19] [20]

En la figura 2.3.1 se observa una pila del protocolo SSL en donde se muestra lo explicado anteriormente.

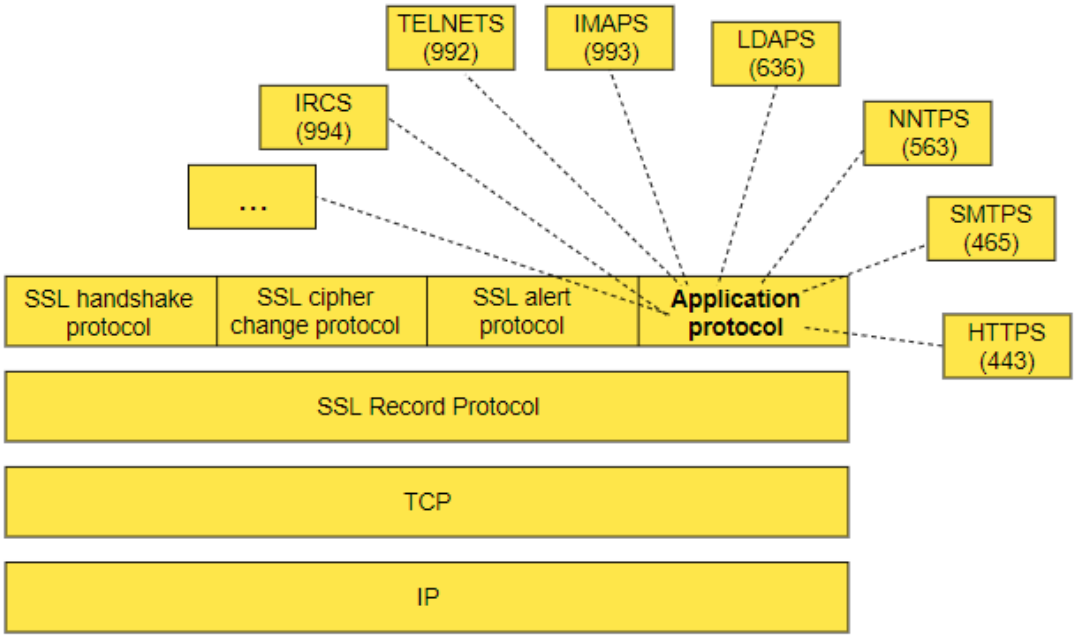

Fig. 2.3.1: Pila del protocolo SSL **[21]**

Después de que SSL quedará obsoleto debido a los avances tecnológicos, surgió el protocolo TLS el cuál no introdujo grandes cambios con respecto al anterior, pero si fueron suficientes como para que no pudieran interoperar. [19]

Para tener una idea genérica de la evolución del protocolo SSL/TLS, en la figura 2.3.2 se observa los cambios más significativos entre versiones. [19] [22] [23] [24]

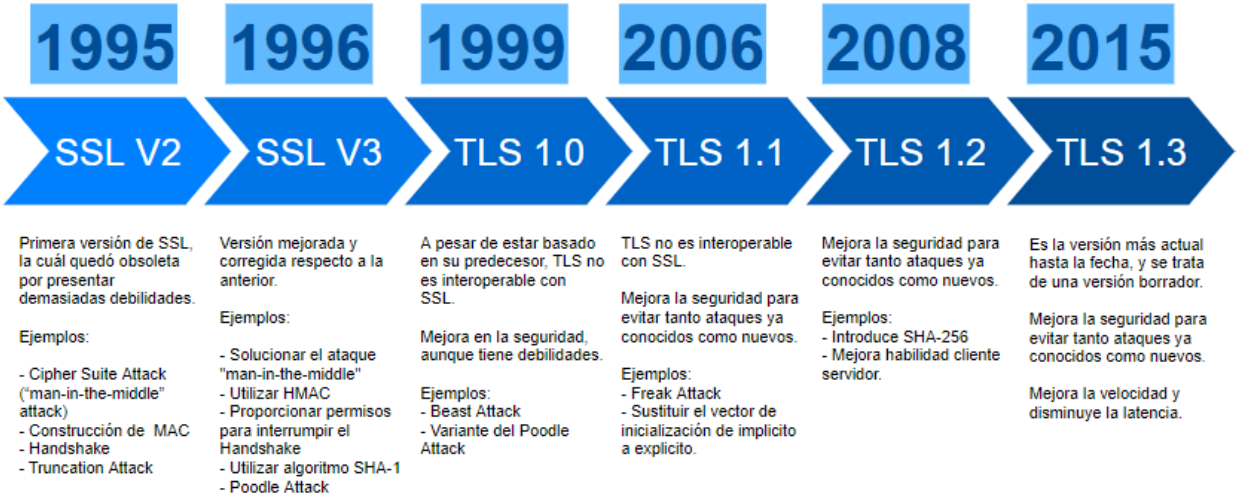

Fig. 2.3.2: Evolución del protocolo SSL/TLS

Como cabe esperar, esto es algo muy importante a tener en cuenta cuando utilizamos cualquier aplicación en remoto. Es por ello que con nuestra herramienta se puede configurar el nivel de seguridad mínimo que se va a soportar según las necesidades de la empresa, de tal forma que evite que un usuario acceda desde un entorno no fiable a una aplicación empresarial, además de impedir posibles ataques por agujeros de seguridad.

2.3.2 IPSEC

IPsec (*Internet Protocol Security*) [3] es un conjunto de protocolos que garantiza las comunicaciones privadas y seguras a través de redes IP (*Internet Protocol*) utilizando la criptografía para ofrecer seguridad. [25]

Debido a que IPsec trabaja en la capa de red del modelo OSI, dispone de una mayor flexibilidad para ayudar a proteger a los protocolos de las capas superiores como puede ser el caso de TCP/UDP.

Como se ha comentado anteriormente, IPsec está formado por un conjunto de protocolos, que son los siguientes:

- AH (*Authentication Header*): Posee autenticación e integridad, validando al remitente y detectando cambios en la transmisión si los hubiere. [26]
- ESP (*Encapsulating Security Payload*): Posee autenticación y cifrado, validando al remitente y cifrando los datos que se envían proporcionando privacidad a la información. [27]

[3] https://www.simplilearn.com/understanding-ipsec-rar37-article

- IKE (*Internet Key Exchange*): Es un protocolo estándar que gestiona claves públicas que se utiliza para asegurar la seguridad en la negociación al realizar conexiones de accesos remotos o VPNs. [28]

Además IPsec admite dos modos de uso, que son: [25]

- Modo Transporte: Sólo se encapsulan los datos que se van a enviar cifrándolos o autenticándolos. Tener en cuenta que aquí no se cifra la dirección IP de modo que esta no puede ser modificada.
- Modo Túnel: Se cifra todo el paquete, cabecera y datos, encapsulándolo en un nuevo paquete IP. Es por ello que en este caso si cambia la IP de origen, a diferencia del modo transporte.

Este protocolo es bastante útil para implementar VPNs y accesos de usuarios remotos a través de una red privada ya que no se necesita realizar ningún cambio por parte del dispositivo del usuario, ni por parte de los programas o protocolos a utilizar. Facilitando su uso en las redes privadas existentes en las empresas.

Al implementar la seguridad en el nivel de IP, una organización puede garantizar una red segura no solo para las aplicaciones que tienen mecanismos de seguridad sino también para las muchas aplicaciones que ignoran la seguridad.

3. FUNCIONAMIENTO DEL SOFTWARE DE PULSE SECURE

3.1 INTRODUCCIÓN

En este capítulo se va a exponer la solución elegida para mejorar el teletrabajo y los accesos a los recursos de una compañía cuando no se encuentran en la oficina. Planteando una sola herramienta que unifique todos los servicios que ya tenga implantada la empresa.

A la hora de plantearse como realizar esta solución, se ha hecho una pequeña investigación para ver que Software se adaptaba mejor a lo que se quiere conseguir. Por ello, después de comprobar la existencia de herramientas como puede Forticlient, Cisco VPN, Pulse Secure y Palo Alto Networks se optó por elegir la solución basada en Pulse Secure, porque es la que mejor se adaptaba a las necesidades de la empresa. Respecto a las compañías anteriormente mencionadas, se descartaron porque disponen de otras funcionalidades, como pueden ser Firewalls, electrónica de red, cloud security…que en el entorno solicitado por la empresa no eran necesarias, porque ya disponían de dichos servicios.

El software de Pulse Secure ofrece diversas funcionalidades que se pueden aplicar al entorno de una compañía. En la siguiente figura se muestra a modo de resumen todas las opciones que ofrece este software, siendo algunas de ellas desarrolladas a lo largo de este proyecto.

Fig. 3.1.1: Funcionalidades de Pulse Secure **[29]**

3.2 Conceptos

Para comprender mejor el funcionamiento del servicio ARU en la consola de administración de Pulse Secure, se va a explicar los conceptos más relevantes e imprescindibles que permitirá realizar las configuraciones necesarias para cumplir las necesidades de la empresa.

Con esta herramienta se permite personalizar de manera muy flexible la experiencia de uso de los usuarios remotos, a través de la configuración de varias entidades conceptuales básicas. Estas son: Roles, Recursos, Dominios de autenticación y Registros.

En la siguiente figura vemos un esquema resumen con el que podemos tener una visión general de cómo funciona dicha herramienta.

Siempre hablando en términos generales, y sin entrar en detalle, para que una acción se realice de forma exitosa el usuario tiene que tener un Rol que va asociado a un Recurso y estos a la vez pertenecer a un dominio de autenticación empresarial, el cual se registra a través de una URL y se valida el acceso a lo solicitado.

Fig. 3.2.1: Esquema conceptual

Entrando en detalle, se va a explicar brevemente cada concepto por separado para comprender la realización de configuraciones que se van a realizar a lo largo de este documento.

3.2.1 Roles

Existen dos tipos de roles, *Admin Role* y *User Role*. En este documento nos centraremos en el rol que interviene con los usuarios de una empresa, *User Role*.

Un *User Role* es un conjunto de tipos de recursos a los que los usuarios pueden acceder. También permite definir el *look & feel* que va a ver el usuario, así como las opciones de la sesión (ej: *session timeouts*). Una forma de administrarlos es creando los roles en función del tipo de recurso al que se pretende acceder: un role para recursos web; un rol para recursos telnet, etc. [30]

Por tanto, lo primero que debe tener nuestra configuración es un *User Role*, configurado con los tipos de recursos a los que queremos dar acceso a los usuarios.

Se pueden especificar requisitos de seguridad basados en diferentes elementos para restringir que los usuarios tengan visibilidad de los recursos de un role. Esta configuración se puede hacer en la propia definición del role (*role restrictions*) o mediante reglas en el dominio de autenticación (*role mapping rules* en el *authentication realm*).

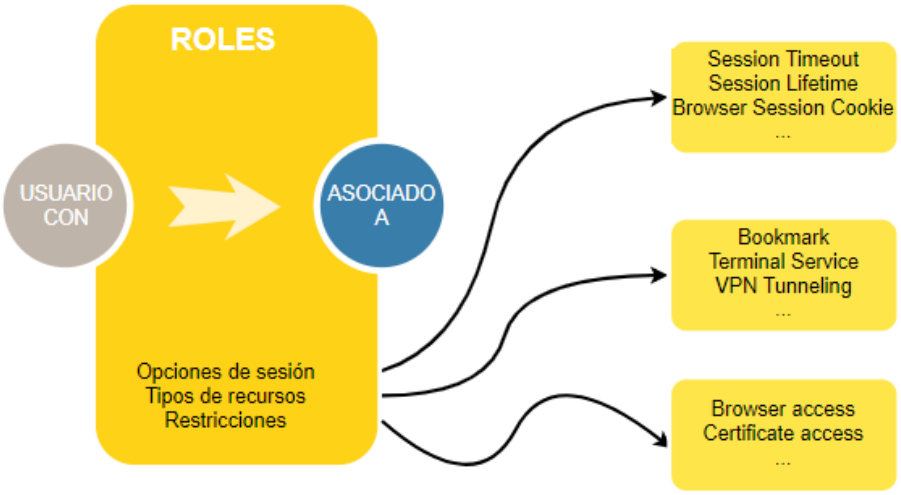

Fig. 3.2.2: Esquema del Rol

3.2.2 Recursos

Una vez que tenemos un Rol, hay que definir los recursos. Para ello se utilizan los *Resource Profile*, que permite una configuración más específica. En este caso, hay que configurar tres cosas: [30]

- Se define los recursos a los que se quiere acceder (ej: la Intranet corporativa)
- Se vinculan los recursos a los roles
- Se definen los marcadores (bookmark)

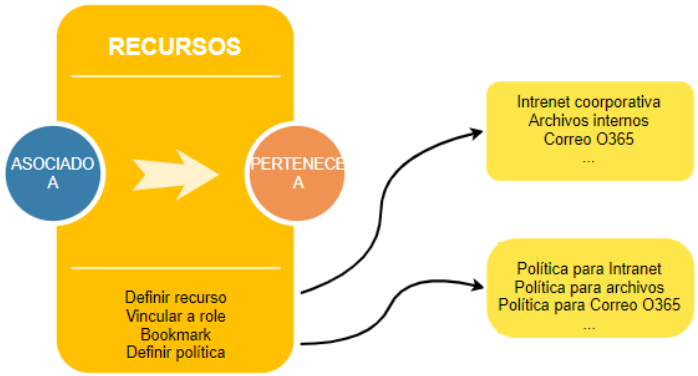

Fig. 3.2.3: Esquema de los Recursos

También hay que definir la política del recurso, *Resource Policy*, que son las reglas del sistema que especifican acciones y recursos concretos para unas determinadas características de acceso remoto. Por ejemplo, se puede permitir o denegar el acceso de un usuario a un recurso en función de diversos factores.

Las políticas se definen en *Resource Policies*. Al crear un recurso en *Resource Profile* se crea una política por defecto para permitir el acceso, que puede ser suficiente si no se requiere una configuración muy específica. [30]

3.2.3 Dominio de autenticación

El acceso de los usuarios se controla con un dominio de autenticación, *Authentication Realm*, que es un grupo de recursos de autenticación.

En primer lugar hay que definir el Servidor de autenticación, *Authentication Server*, que es la base de datos con las credenciales de usuario, que van a permitir verificar que el usuario es quién dice ser. Se pueden utilizar diversos tipos de servidores de autenticación: local, radius, LDAP, Directorio Activo, etc. [30]

Después se configura el dominio, *Realm*, en el que se definen las siguientes características: [30]

- Se vincula al *Authentication Server* con el que queremos verificar las credenciales de usuario.

- Se definen las políticas de autenticación, *Authenticacion Policy*, que es el control de acceso a la página de inicio de sesión. Es un conjunto de reglas que controlan si hay que presentar una página de inicio de sesión a un usuario. Por ejemplo especificar IP origen, longitud de la contraseña, uso de certificado, tipo de navegador, políticas de host checker, etc.

- Se establecen las condiciones para mapear usuarios a roles, *Role-mapping rules*. Son las condiciones que un usuario debe cumplir para mapear a los roles, estas pueden estar basadas en *username*, certificado, etc.

Fig. 3.2.4: Esquema del Dominio de autenticación

3.2.4 Registro

Por último, se configuran políticas del proceso de registro, *Sign-in Policies*: [30]

- Se define una URL en la que los usuarios se registrarán en el servicio.
- Se personaliza la web de registro, *Sign-in pages*, que visualizará el usuario.
- Se especifica que dominios de autenticación aplican a cada URL y web.

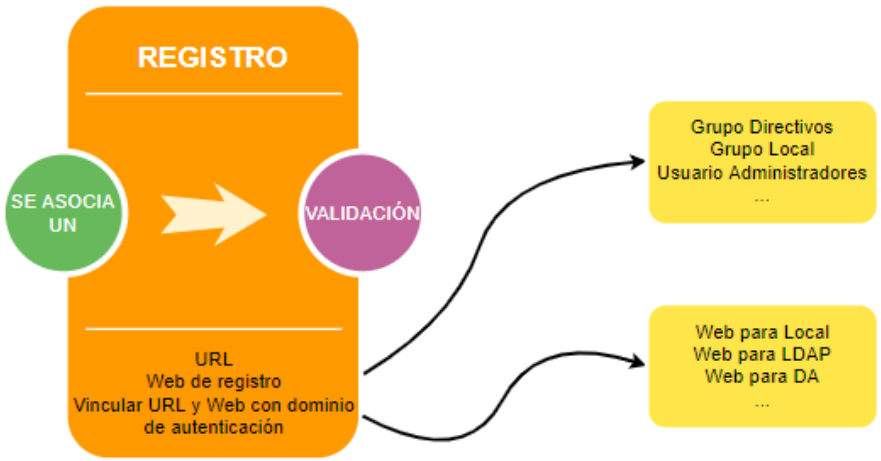

Fig. 3.2.5: Esquema del Registro

3.2.5 Esquema completo

Para tener una imagen general de todos los elementos explicados anteriormente, en la figura 3.2.6 se muestra un diagrama de la relación entre todos los elementos descritos.

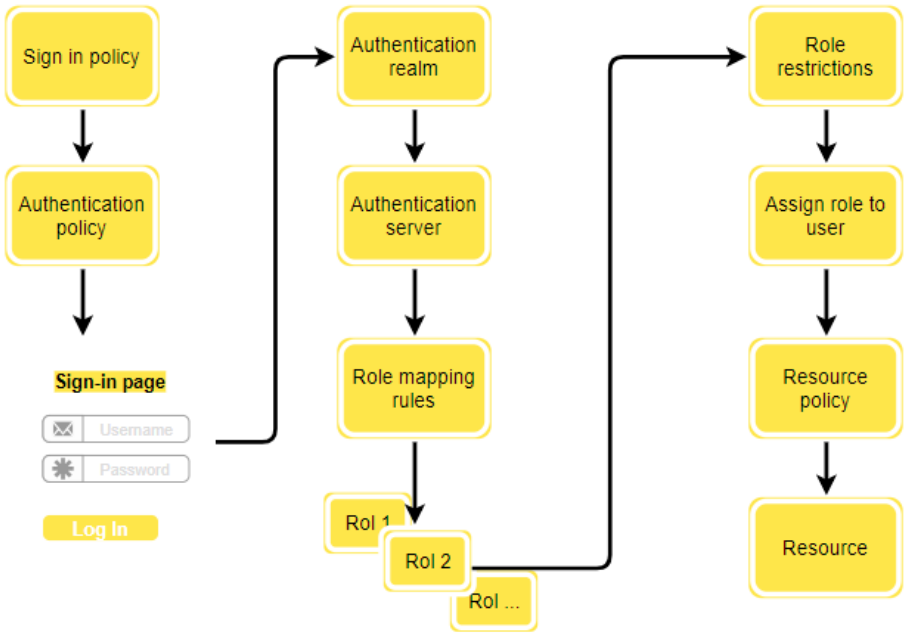

Fig. 3.2.6: Diagrama completo de los elementos implicados

3.3 Funcionalidades

A continuación se va a configurar en Pulse Secure algunos de los recursos descritos anteriormente, obteniendo así un primer contacto con la herramienta. En los próximos capítulos se profundizará más sobre estas funcionalidades.

3.3.1 Usuarios locales

Para configurar esta autenticación, hay que ir a la página de administración del entorno e ir a **Authentication/Auth. Servers/Local Users.** Una vez dentro, hay que añadir a los usuarios locales. Para ello entramos dentro de **Users/New**.

Se rellenan los datos según los proporcionados por la empresa y se guardan los cambios.

Fig. 3.3.1: Captura de usuarios locales

Fig. 3.3.2: Captura añadir usuarios locales

Como se ha explicado en el apartado anterior, se necesita asociar un rol y un realm a los usuarios para que estos tengan acceso a los recursos que más adelante se van a configurar. Esto lo veremos en los próximos capítulos y se explicará cómo funciona.

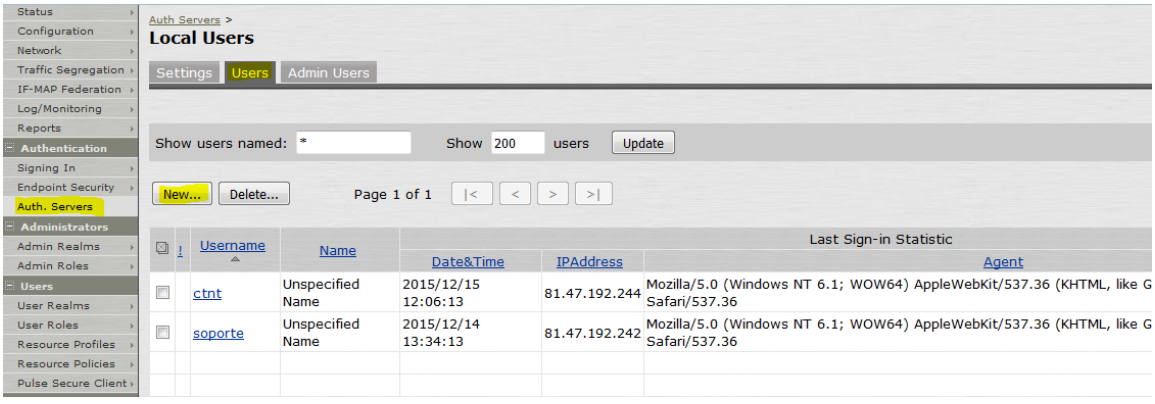

Fig. 3.3.3: Captura usuarios locales

3.3.2 Usuarios de directorio activo

Para configurar esta autenticación, hay que ir a la página de administración del entorno e ir a **Authentication/Auth. Servers/** y crear un nuevo servidor de DA, por ejemplo:

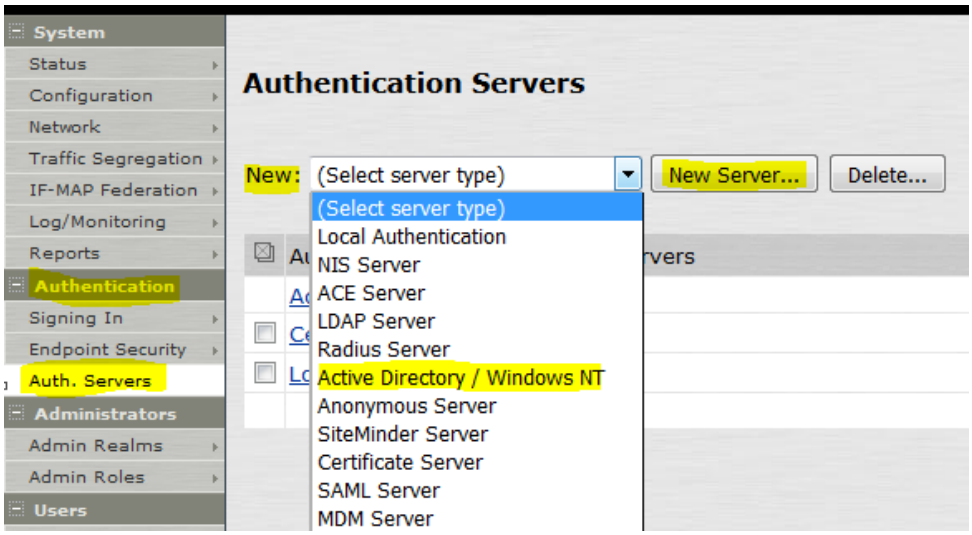

Fig. 3.3.2: Creación servidor Directorio Activo

Se rellenan los datos según los proporcionados por la empresa y se guardan los cambios.

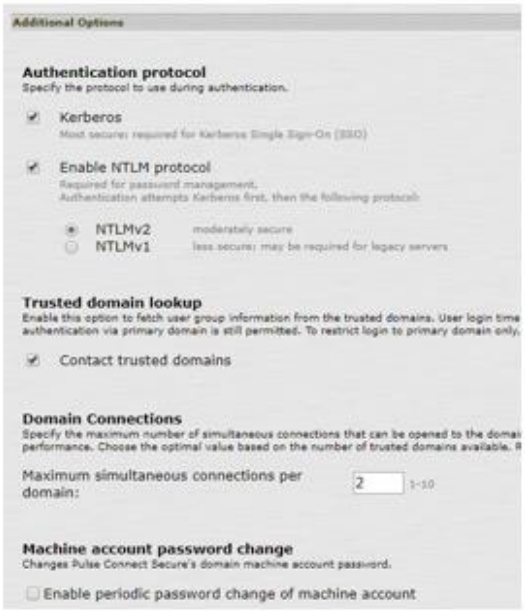

Fig. 3.3.3: Configuración del DA

Al igual que sucede en el caso de los usuarios locales, aquí también se necesita asociar un rol y un realm.

Respecto a los usuarios, al tratarse de un directorio activo los usuarios se añaden automáticamente según van accediendo a la plataforma. No es como en el caso de los usuarios locales que hay que crearlos.

3.3.3 Acceso por VPN

Para habilitar el acceso por VPN, hay que ir a la página de administración del entorno e ir a **Users/Resource Policies/VPN Tunneling** y aquí se deben configurar tres opciones para el correcto funcionamiento de los recursos una vez levantado el túnel. Estas son: el control de acceso, el pool de redes y Split-tunneling.

El control de acceso consiste en controlar los recursos a los que los usuarios pueden acceder cuando están utilizando VPN Tunneling. Para ello se crea una nueva política que defina dichos permisos.

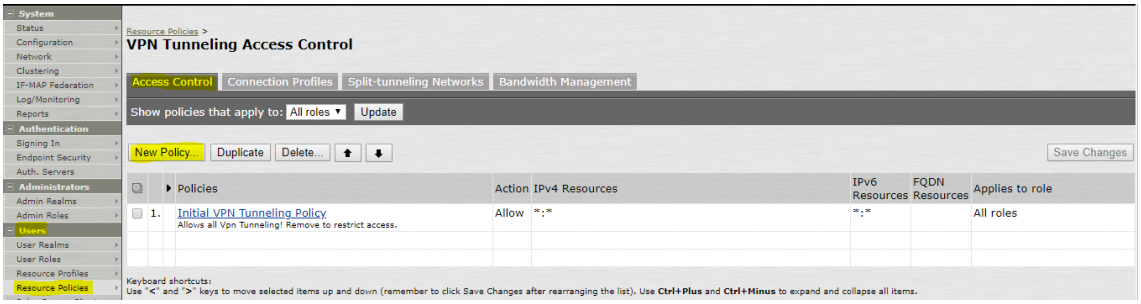

Fig. 3.3.4: Política del Control de acceso

Al crear la política, se debe especificar las redes a las que se va a tener o no acceso, ya sea sólo IP o el protocolo e IP. En caso de que no se quiera restringir ningún acceso, salvo el establecido en la intranet, se pondrá un *. Finalmente se selecciona a quienes se les va a aplicar la política (los roles) y se indica si se va a permitir o denegar el acceso a las redes definidas.

Fig. 3.3.5: Política de control de acceso

Para el pool de redes, se debe configurar la pestaña *Connection profile*. Aquí se define el rango perteneciente a la red de la empresa que estará reservado para las conexiones por VPN. Cuando un usuario levante un túnel se le asignará una IP del rango aquí definido.

Opcionalmente se puede configurar el *Split Tunneling*. Habilitando esta opción se consigue que se securice todas las redes IP definidas y vayan a través del túnel VPN. El resto irá por fuera del túnel. Un ejemplo sería el mostrado en la siguiente figura.

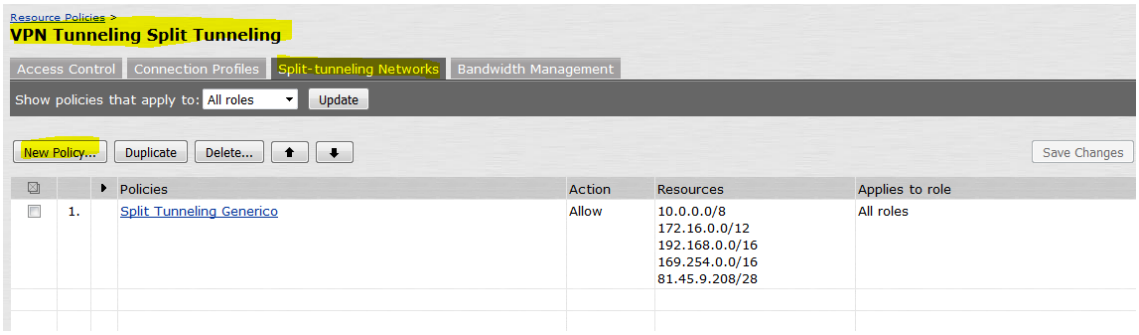

Fig. 3.3.7: Configuración genérica de Split Tunneling

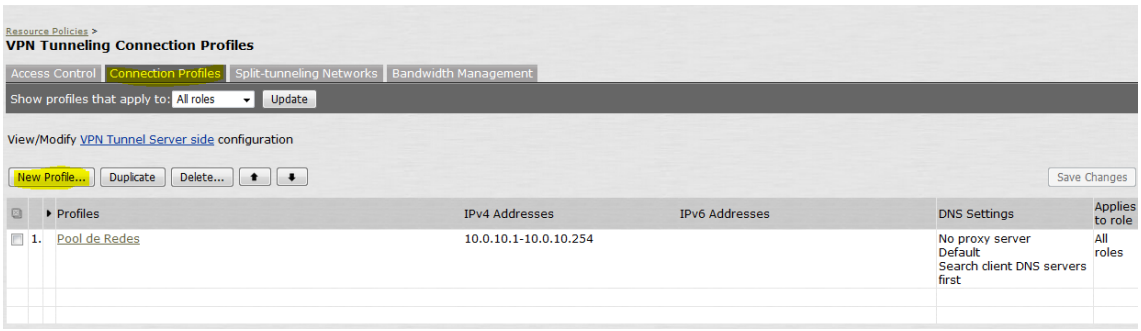

Fig. 3.3.6: Pool de redes

3.3.4 Opciones para los protocolos de seguridad

En la siguiente figura se observan los apartados sobre SSL/TLS. Dependiendo de la seguridad establecida en los ordenadores personales y de trabajo, así se seleccionará una u otra opción. [30]

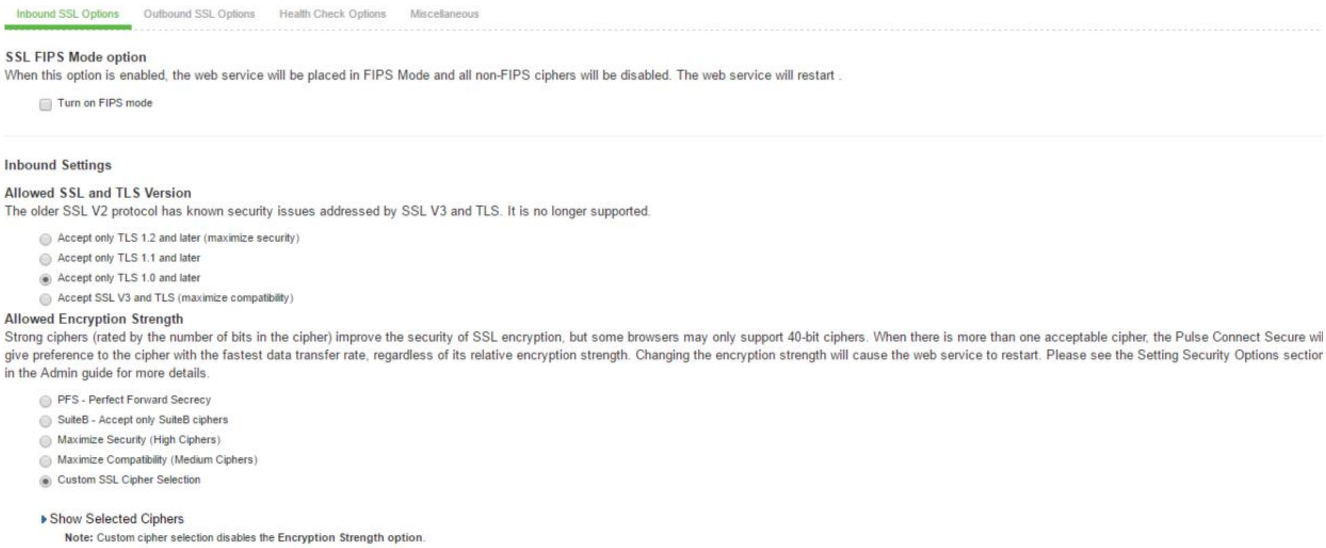

Fig. 3.3.8: Apartado de SSL/TLS

3.3.5 Host Checker

Se va a dedicar un apartado a la seguridad que hay que tener previo paso a realizar la conexión por VPN previo establecimiento de la conexión por VPN.

Es importante que nuestros equipos personales con los que vamos a acceder a la red interna de la empresa no estén comprometidos ni infecte con algún virus a los equipos allí conectados. Ya sea por desconocimiento o por descuido, los dispositivos de los usuarios, como puede ser el portátil o el móvil, no tienen implantados unos requisitos de seguridad que a diferencia de los que se encuentran en la oficina si tienen. Es por eso que se va a estudiar el Host Checker. [31]

Esta tecnología está basada en la arquitectura y estándares de TNC (*Trusted Network Connect*) proporcionando un enfoque integral para evaluar la fiabilidad de los elementos finales. La arquitectura de TNC está diseñada para desarrollar estándares y tecnologías establecidos, como pueden ser IEEE 802.1X, RADIUS, IPsec, EAP y TLS / SSL.

El Host Checker es un agente que se despliega en el lado del cliente para realizar las comprobaciones de estado y seguridad de los equipos que intentan conectarse a otro dispositivo concreto. Esta es la propuesta de Pulse Secure como solución para evitar que se conecten a la red privada de la empresa equipos carentes de seguridad, obsoletos o con un malware que haga vulnerable la red. De modo que con esta herramienta se puede seleccionar a qué tipo de equipo se le permite la conexión, así como las características que debe cumplir. Combinando las diferentes opciones que incluye esta opción se puede ser más o menos restrictivo con los accesos del exterior, además de elegir a que se deja acceder según qué opciones cumpla. Como cabe esperar este es uno de los puntos fuertes respecto a seguridad que ofrece Pulse Secure.

Una vez puestos en contexto se va a mostrar en dos tablas las compatibilidades que existen con la última versión del Host Checker y los permisos que hay que tener para instalar y ejecutar ActiveX o JAVA, necesarios para desplegar el host checker la primera vez que se realice la conexión. [31]

TABLA 3.2.1
COMPATIBILIDADES CON SISTEMAS OPERATIVOS Y NAVEGADORES

PLATFORM	Operating System	Browser and Java Environment
Windows	• Windows 10 on 32 bit or 64 bit platforms • Windows 8 and 8.1 on 32 bit or 64 bit platforms • Vista Enterprise/Ultimate/Business/HomeBasic/Home Premium with Service Pack1 or 2 on 32 bit or 64 bit platforms • Windows 7 Enterprise/Ultimate/Professional/HomeBasic/Home Premium on 32bit or 64 bitplatforms (6.5R2 and above) • XP Professional with SP2 or SP3 on32 bit or 64 bit • 2000 Professional SP4 • XP Home SP3 • XP Media Center 2005 • Windows 2003 server SP2, 32bit and 64 bit	• Internet Explorer 8.0 * • Internet Explorer 7.0 * • Internet Explorer 6.0 * • Firefox 3.5 • Firefox 3.0 • Firefox 2.0 • Sun JRE 5/1.5.07 and above • Microsoft JVM – for Windows 2000 (*Whereverapplicable)
Mac	• Mac OS X 10.6, 32 bit and 64 bit • Mac OS X 10.5.x, 32 bit and 64 bit • Mac OS X 10.4.x, 32 bit only • Mac OS X 10.3.x, 32 bit only	• Safari 1.2 and above • Sun JRE 5/1.5.07 and above
Linux	• OpenSuse 10.x, 32 bit only • Ubuntu 7.10, 32 bit only • Red Hat Enterprise Linux 5, 32 bit only	• Firefox 2.0 and above

TABLA 3.2.2
PERMISOS NECESARIOS SEGÚN SISTEMA OPERATIVO

	Active X Windows	Active X: Installer Service Windows	Java Windows	Java Mac / Linux
Install Restricted, Power User or Admin	✓	✓	✓	✗
Run Restricted, Power User or Admin	✓	✓	✓	✗

En la siguiente tabla se va a mostrar los tipos de reglas que dispone esta herramienta, dado que su objetivo es realizar políticas para su futuro cumplimiento. Se van a distribuir por tipo de sistema operativo a utilizar. [31]

TABLA 3.2.3
REGLAS COMPATIBLES SEGÚN SISTEMA OPERATIVO

	Windows	Mac	Linux	Solaris
Predefined: Antivirus	✓	✓	✗	✗
Predefined: Firewall	✓	✓	✗	✗
Predefined: AntiSpyware	✓	✓	✗	✗
Predefined: HardDisk Encryption	✓	✓	✗	✗
Predefined: Patch Management	✓	✓	✗	✗
Predefined: OS Checks	✓	✓	✗	✗
Predefined: CVE Checks	✓	✗	✗	✗
Custom: 3rd Party NHC Check	✓	✗	✗	✗
Custom: Ports	✓	✓	✓	✓
Custom: Process	✓	✓	✓	✓
Custom: File	✓	✓	✓	✓
Custom: Resgistry Settings	✓	✗	✗	✗
Custom: NetBIOS	✓	✗	✗	✗
Custom: MAC Address	✓	✗	✗	✗
Custom: Machine Certificate	✓	✗	✗	✗
Custom: Advanced Host Checking	✓	✗	✗	✗
Custom: Statement of Health	✓	✗	✗	✗

A modo de ejemplo se va a profundizar en las reglas más utilizadas. [31]

3.3.5.1 Antivirus

Como se muestra en la siguiente imagen, podemos seleccionar como criterio que se validen a los usuarios si tienen un antivirus:

- Cualquiera soportado por Pulse Secure (Products supported by Endpoint Security Assessment Plugin ESAP 3.2.5). [32]
- De un fabricante especifico, incluyendo todas sus versiones soportadas.
- De un fabricante y versión especifica.

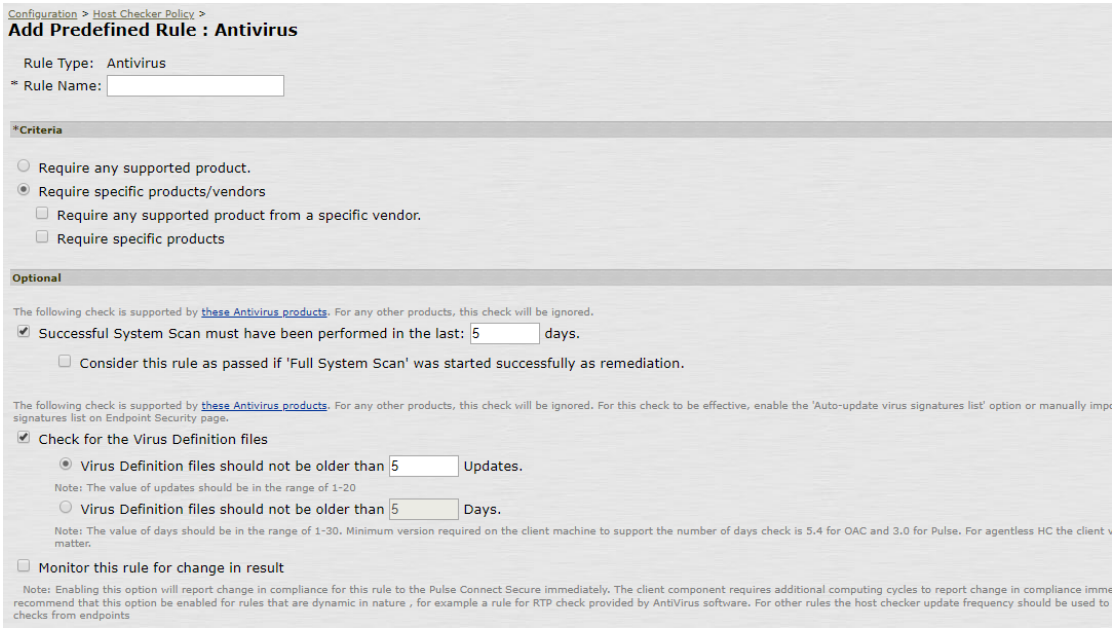

Fig. 3.3.9: Ajustes regla antivirus del Hoste checker

Adicionalmente se puede añadir las siguientes comprobaciones:

- El examen del antivirus fue exitoso en los últimos ‘x’ días.
- Los archivos de definición no deben tener menos de ‘x’ actualizaciones o días.
- Ejecutar esta regla continuamente.

Una vez seleccionado el tipo de antivirus que vamos a exigir que tengan los usuarios, se debe seleccionar una opción para solventarlo en caso de no pasar el test. Hay tres opciones a realizar: [32]

- Descargar el último archivo disponible desde la web del proveedor si es compatible con ESAP 3.2.5.
- Activar la protección en tiempo real si es compatible con ESAP 3.2.5.
- Ejecutar un examen del antivirus en tiempo real si es compatible con ESAP 3.2.5.

Fig. 3.3.10: Reparación en caso de fallo

3.3.5.2 Firewall

Con esta regla se comprobará si existe o no firewall. Además tiene los mismos criterios que en el caso anterior (enfocado a firewalls), a diferencia de que sólo se puede realizar la opción de ejecutar esta regla continuamente.

Como opción para solventarlo en caso de fallo, se puede habilitar el firewall en el momento del testeo de la regla.

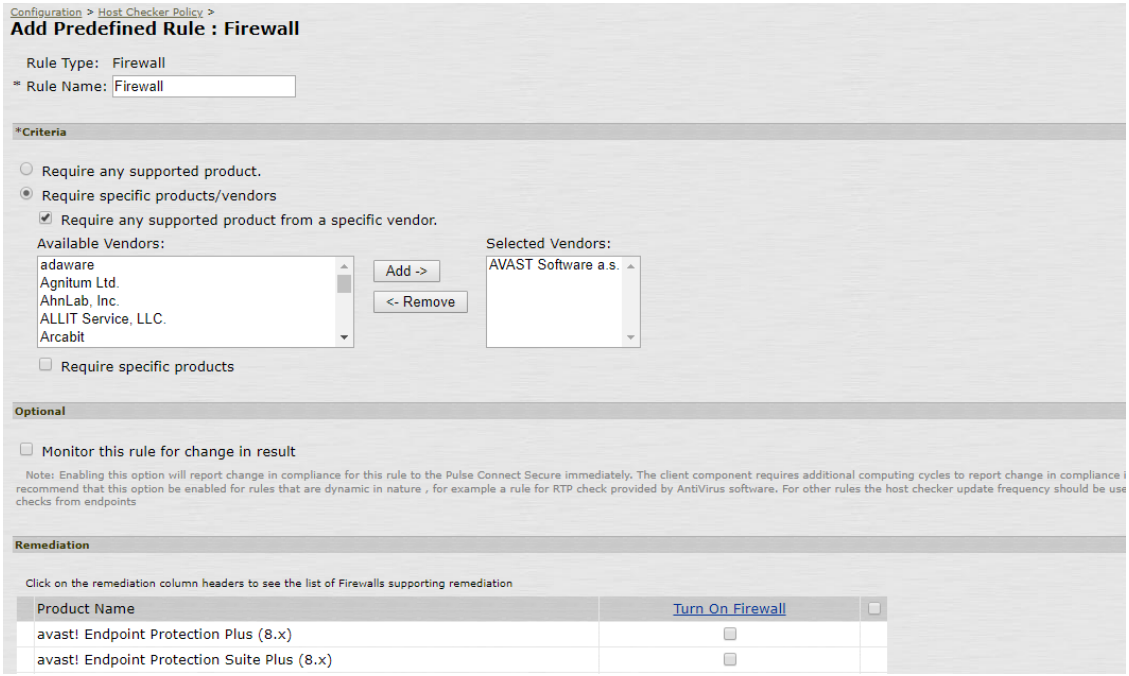

Fig. 3.3.11: Ajustes regla firewall del Host checker

3.3.5.3 OS Check

Esta regla permite denegar el acceso a recursos dependiendo del sistema operativo y *service pack* del que disponga.

Fig. 3.3.12: Ajustes regla sistema operativo del Host checker

Tras describir las funcionalidades aportadas por esta herramienta vemos que es una elección muy completa respecto a lo que se quería conseguir. Se ha propuesto un software con el cual se puede gestionar y configurar diferentes tipos de accesos y conexiones remotas. Además cuenta con una gestión sobre la seguridad que deben acatar los usuarios que accedan de forma externa a la intranet, ejerciendo la obligación de cumplir los requisitos aportados por el host checker.

Como se ha indicado a lo largo del documento, se comprueba que el software cuenta con una interfaz de fácil manejo y la cual soporta todos los sistemas operativos, además de diferentes tipos de integraciones tanto de directorio como de accesos webs o autenticaciones.

No obstante, en el siguiente capítulo se van a exponer diferentes escenarios cuya solución estará basada en Pulse Secure.

4. CASOS PRACTICOS

Una vez explicado en qué consiste este servicio, cómo funciona y se gestiona, se va a recrear una serie de casos prácticos en los que este servicio se verá implicado. Con ello se verá que el servicio ARU ofrece, no solo una solución al acceso remoto sino seguridad y fiabilidad al realizar las comunicaciones a través de la herramienta Pulse Secure.

A continuación se van a exponer diferentes escenarios en los que se van a explicar casos prácticos sobre el uso de esta herramienta y resolución de problemas encontrados. Dicho orden irá desde algo básico y común hasta algo complejo en el que se requiere de ciertos conocimientos técnicos.

En todos los escenarios que se van a describir se parte de una empresa que necesita una solución para realizar su trabajo en remoto y tener acceso a los recursos internos de la misma, teniendo en cuenta la importancia de que toda comunicación sea segura, se lleve un control de los accesos de los empleados y se evite tener que utilizar diferentes herramientas.

Por esta razón se propone como solución utilizar la herramienta de Pulse Secure, ya que ofrece un acceso remoto unificando todas las necesidades que tenga la empresa en un solo recurso. A lo largo de los diferentes casos prácticos se va a analizar los motivos que han llevado a dar esa solución y no otra.

Antes de describir los escenarios se va a poner en conjunto la configuración inicial que requiere Pulse Secure para establecer la conexión herramienta remota ⇄ red interna empresa.

4.1 Pasos previos

Primero se configuran los accesos básicos para dar las credenciales de administrador de Pulse y la de los usuarios finales. Algo importante a tener en cuenta es que el acceso de administrador a la herramienta de Pulse, sólo se puede realizar desde la red interna de la empresa, para evitar que se acceda desde fuera como un enlace público.

Fig. 4.1.1: Usuario administrador de la plataforma

Como se observa en la siguiente imagen, tenemos configurado el puerto interno correspondiente con una IP dentro del rango de la empresa y que se encuentre libre. Desde este momento, esta IP sólo será para el acceso del ARU.

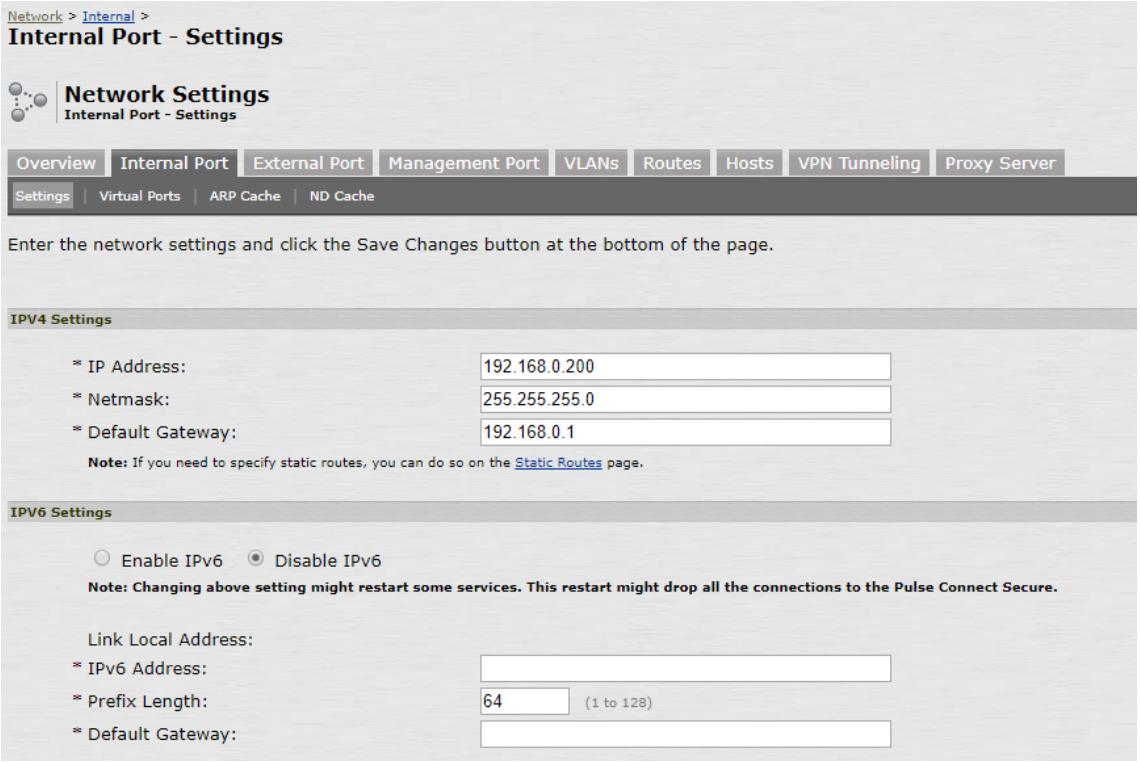

Fig. 4.1.2: Configuración del puerto interno

A continuación hay una captura en la que está creado tanto el acceso web al usuario admin como a los usuarios básicos. Esto se puede modificar en cualquier momento dependiendo de si se quiere tener una página de inicio diferente para según que grupos departamentales. Posteriormente se irán asociando los usuarios a los recursos y de ello dependerá lo que se muestre en la página principal de pulse.

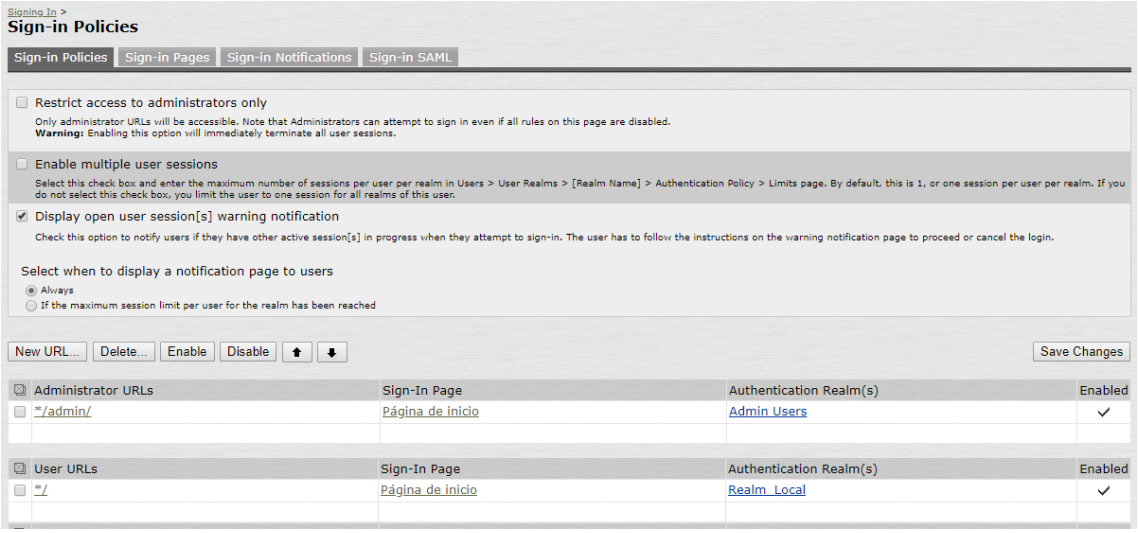

Fig. 4.1.3: Accesos web para el administrador y para los usuarios

En la figura 4.1.4 se pueden apreciar las diferencias en las páginas de inicio.

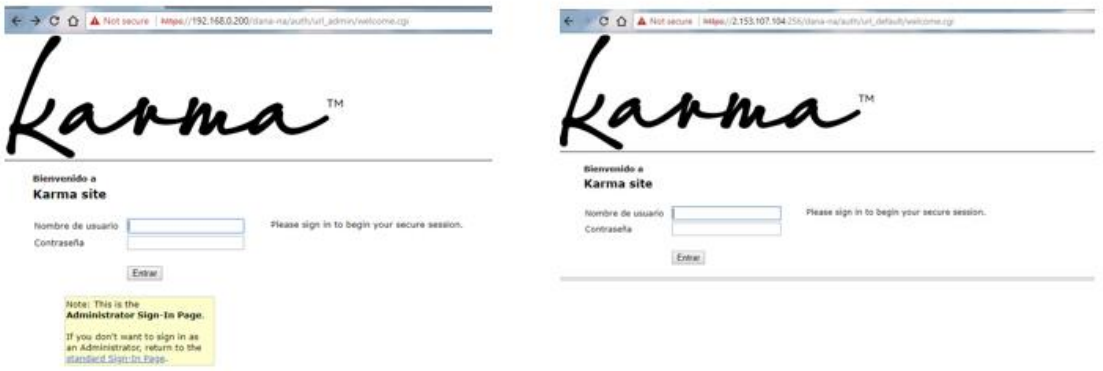

Fig. 4.1.4: Acceso administrador y Acceso usuarios

Respecto a las *skins* mostradas, ambas se pueden modificar. Tanto el texto que aparece como el logo/colores, son opcionales y se pueden ajustar a las necesidades del cliente.

4.2 Escenario 1. Caso básico.

Los trabajadores de una compañía de contenidos digitales, por razones de movilidad y horario, tienen que trabajar a distancia o fuera del horario laboral. Como consecuencia de estas necesidades, la empresa debe establecer una conexión segura a las herramientas que usan sus trabajadores a través de la red interna.

Al tratarse de una pequeña empresa no dispone de un directorio activo, en tal caso lo que solicita es que se creen 10 usuarios locales, que posteriormente se agruparan según la función que

desempeñan en la empresa. Con esta agrupación se podrá determinar a qué recursos accede cada usuario.

Se necesita que algunos trabajadores externos puedan acceder a una herramienta de edición web, pero sin tener acceso a las unidades de red internas por contener elementos confidenciales. Este grupo se denomina “freelance”.

Por otro lado, se requiere que un grupo de trabajadores pueda acceder a un *Terminal Service* donde se encuentra las bases de datos de uso interno (hemeroteca). Por tanto, es importante que su acceso sea restringido sólo al grupo “analytics”.

Por último, todos los usuarios deben poder acceder al correo de la empresa, que en este caso es un web mail.

Resumiendo, las condiciones a cumplir son:

- Son usuarios locales, con determinada seguridad en la contraseña.
- Habilitar el acceso a un recurso web.
- Habilitar el acceso a un *Terminal Service* donde tienen instalado un programa de uso interno.
- Habilitar el acceso al correo de empresa.
- Existen diferentes grupos departamentales los cuales tienen unos recursos particulares y no puede acceder personal ajeno a dicho departamento.
- Se debe exigir que el dispositivo desde donde se vaya a acceder a la red interna cumpla una serie de requisitos de seguridad para evitar posibles fugas.
    - Sistema Operativo Windows 7
    - El test del antivirus esté correcto de hace 2 días y además pasa el test exhaustivo.

Se va a estudiar cómo con el acceso remoto unificado se puede cumplir las peticiones descritas de forma rápida, eficaz y segura. Tener en cuenta que dentro de una opción hay muchas combinaciones posibles y que esto se puede ir adaptando a los cambios que realice la empresa o a las nuevas necesidades que vayan surgiendo, puesto que la herramienta es flexible al respecto. Debido a esto, no solo se mostrará la solución aportada para este escenario sino que se va a explicar que otras opciones disponemos en caso de querer utilizarlo en un futuro.

Se va a comenzar por crear a los usuarios locales y a configurar las características que debe tener la contraseña de cada usuario.

Para diferenciar mejor el acceso de los usuarios se pondrá como nombre de usuario el número de matrícula de cada uno. Esto facilitará la lectura de los logs, así como las asignaciones que se realicen en un futuro.

Primero hay que ir a **Auth Servers** y seleccionar el tipo de servidor que vamos a crear. En este caso se selecciona **Local Authentication**.

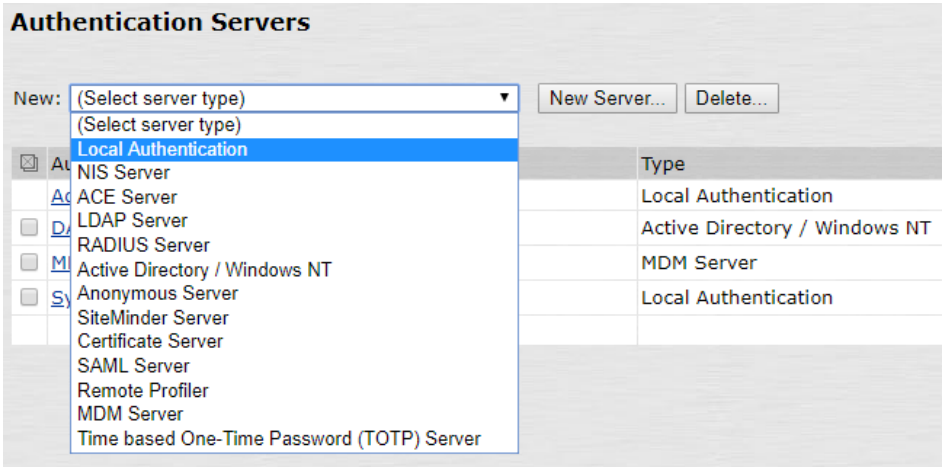

Fig. 4.2.1: Configuración usuarios locales de la empresa

A la hora de crear el servidor local, se va a configurar tanto las características que debe cumplir las contraseñas como la creación de los diferentes usuarios. En las siguientes figuras se observa tanto el servidor como los usuarios:

Fig. 4.2.2: Ajustes de la configuración del servidor local

Fig. 4.2.3: Usuario nuevo y error de contraseña

	Username	Name	Last Sign-in Statistic		
			Date&Time	IPAddress	Agent
	dg146	Antonio Perez	2018/06/02 13:25:18	47.60.38.181	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chro Safari/537.36
	dg210	Ernesto Gracia	2018/06/02 12:56:49		
	dg380	Carlos Jimenez	2018/06/02 12:56:09		
	dg523	Alicia Perez	2018/06/02 12:47:42	47.60.38.181	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chro Safari/537.36
	dg534	Maria del Campo	2018/06/02 12:57:10		
	dg776	Patricia Garcia	2018/06/02 12:56:33		
	dg777	Felipe Lopez	2018/06/02 13:26:38	47.60.38.181	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chro Safari/537.36
	dg888	Lucia Sanchez	2018/06/02 12:55:21		
	dg906	Thalia Lillo	2018/06/02 12:57:38		
	dg910	Jorge Diaz	2018/06/02 11:24:09		

Fig. 4.2.4: Usuarios locales

Finalmente, obtenemos el servidor ‘Usuarios Locales’ con todos los usuarios de la empresa.

Fig. 4.2.5: Servidor local

Se procede a asignar un Realm y un Rol perteneciente a cada grupo o grupos según sea necesario. Con ello se podrán realizar mapeos para dar o no permisos a los diferentes recursos a configurar.

A modo de ejemplo, se crea el Rol de Freelance para indicar a qué recursos van a tener acceso los usuarios freelance que se les asignen este rol. Se habilita el acceso Web y el VPN Tunneling.

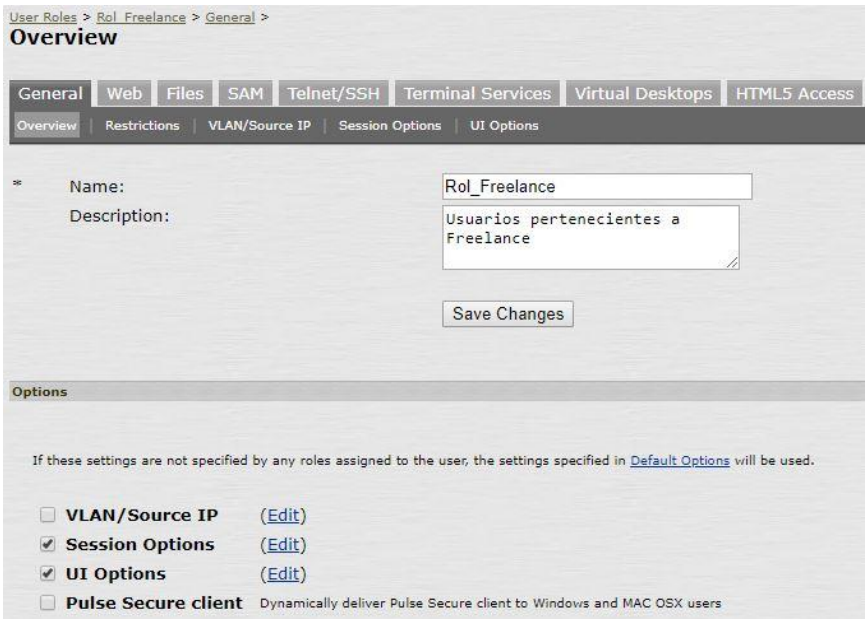

Fig. 4.2.6: Creación del Rol_Freelance

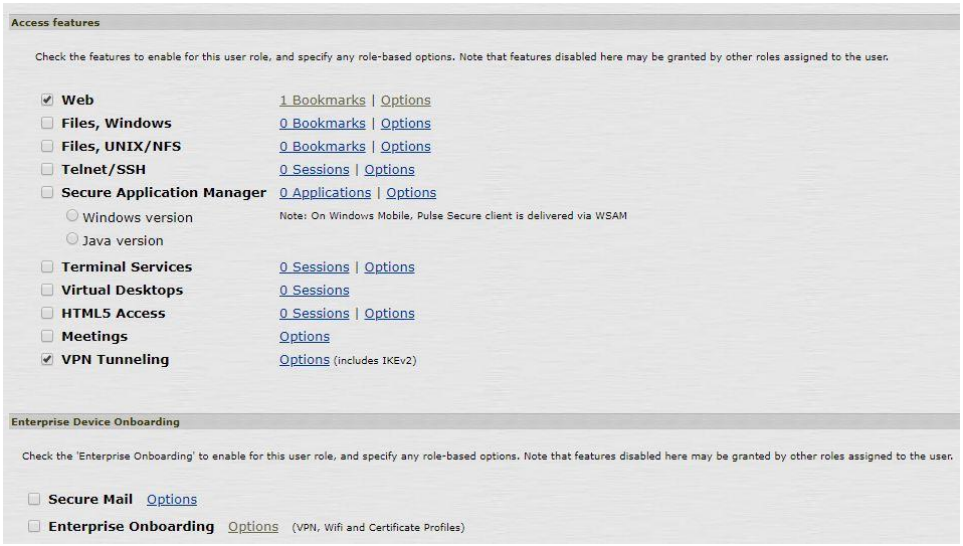

Fig. 4.2.7: Creación del Rol_Freelance

Finalmente se crean el resto de roles necesarios, en donde Rol_Analytics tiene habilitado Terminal Services y VPN Tunneling y Rol_Generico tiene web y VPN Tunneling.

Fig. 4.2.8: Creación de todos los roles

A continuación se crean los Realms correspondientes a los roles para el correcto funcionamiento de los usuarios.

Como se ha indicado al principio, se requiere que los usuarios se agrupen por sus funciones. Para realizar esto se van a crear reglas en el Realm (*Role Mapping*) para asignar a cada usuario el Rol que le corresponde. De esta forma, cuando el usuario se autentique con sus credenciales automáticamente le aparecerán los recursos que tiene asignados en su rol o roles.

Se crea el Realm genérico denominado 'Realm_Local' el cual se le asignará a todos los usuarios pertenecientes al servidor 'Usuarios Locales'.

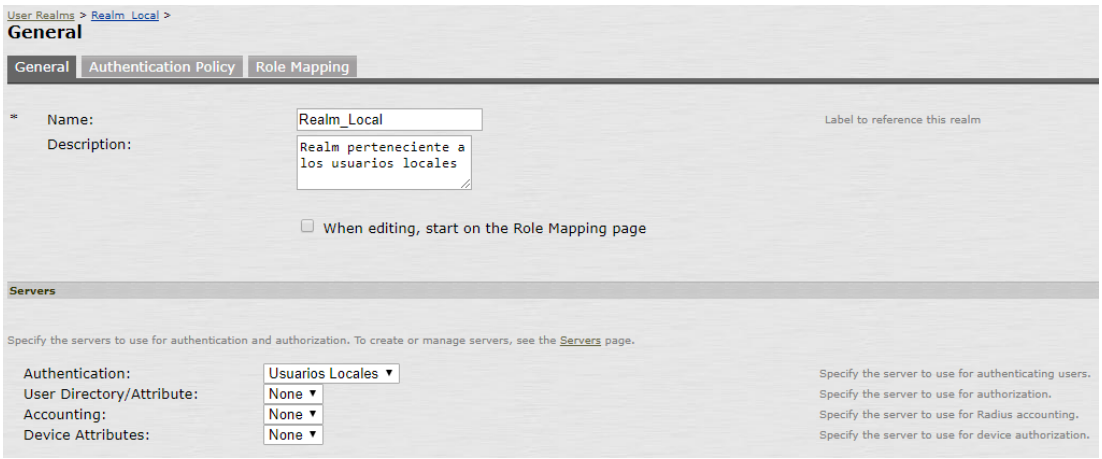

Fig. 4.2.9: Creación del Realm_Local

Como se puede observar a continuación, se han creado 3 reglas diferentes. Estas se diferencian por los nombres de usuarios, es decir, según sea el nombre de la persona que se conecte así se le asignará un rol u otro. Tener en cuenta que sólo en la regla genérica (la que es con *) se detiene la asignación de roles, pues en este caso todos los usuarios deben tener acceso al correo electrónico (se corresponde con el rol 'Rol_Generico').

Los usuarios pertenecientes a Analytics o a Freelance, se le asignará tanto su respectivo rol como el 'Rol_Generico' pues cumplen ambas reglas.

Fig. 4.2.10: Creación del Role Mapping

Finalmente se obtiene el realm.

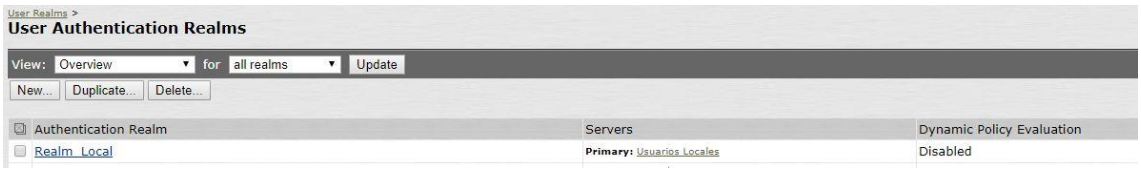

Fig. 4.2.11: Creación del Realm_Local

Una vez que se tiene las configuraciones básicas, se va a proceder con la creación de los diferentes recursos. En este caso son:

1. Correo de empresa
2. Terminal Services
3. Bookmark tipo Web

1. Correo de empresa

Para el caso del web mail se va a utilizar un servicio de correo electrónico de Go Daddy. Esta plataforma de cloud, además de realizar registros de dominios y alojamiento web, ofrece un servicio de correo sin la necesidad de disponer de un hosting. Con ello se obtiene un correo corporativo vinculado al dominio de la empresa. [33]

Para ello, se va a crear un bookmark del tipo *Custom* y va a estar asignado al rol que incluye a todos los usuarios pues en este caso no hay distinción por grupos. Este rol es 'Rol_Generico'.

Se crea el Bookmark añadiendo la url del correo y habilitando el Autopolicy que se crea automáticamente.

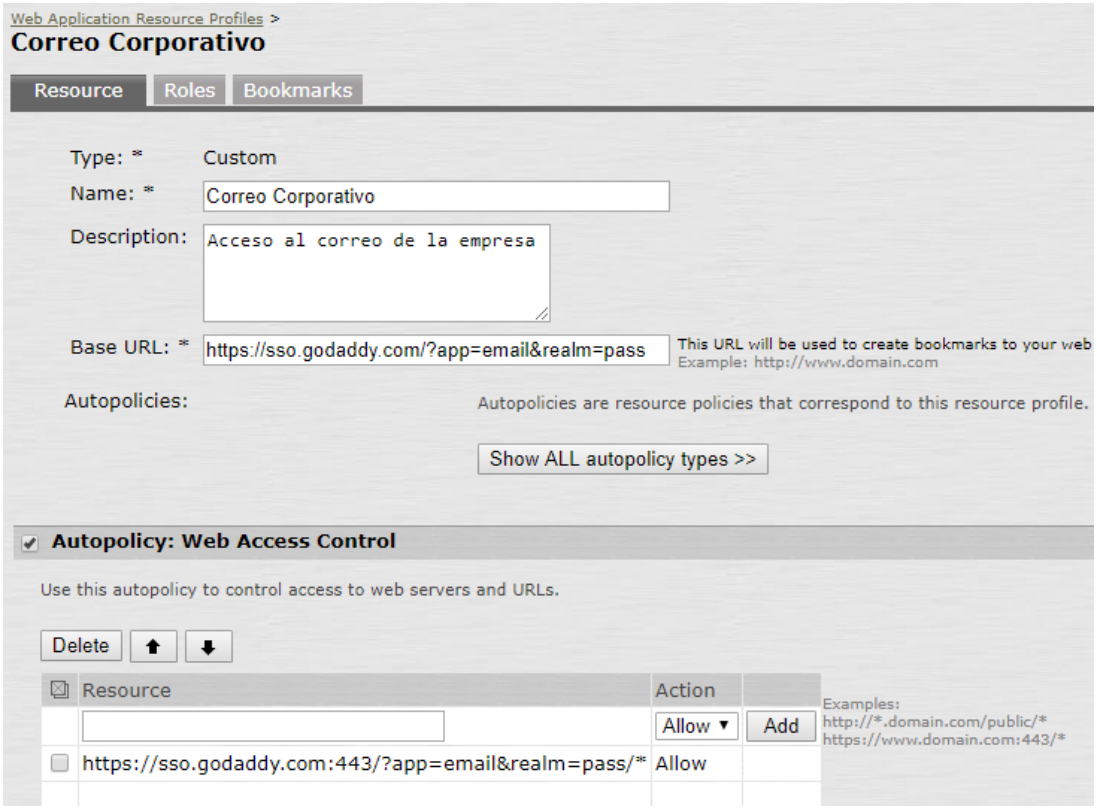

Fig. 4.2.12: Configuración acceso al correo de empresa

Se asigna al rol deseado y directamente se genera el Bookmark que se mostrará cuando se inicie sesión:

Fig. 4.2.13: Asignación al rol genérico

Fig. 4.2.14: Bookmark para el acceso al correo

Una vez está el correo configurado se procede a comprobar si se accede correctamente. Para ello nos conectamos con nuestra IP pública e introducimos las credenciales de un usuario de 'Oficinas', por ejemplo, dg210.

Fig. 4.2.15: Página principal del usuario *dg210*

Como se observa en la captura anterior, tenemos como marcador web 'Correo Corporativo'. Al entrar en ese enlace nos lleva al correo de la empresa tal y como se muestra a continuación.

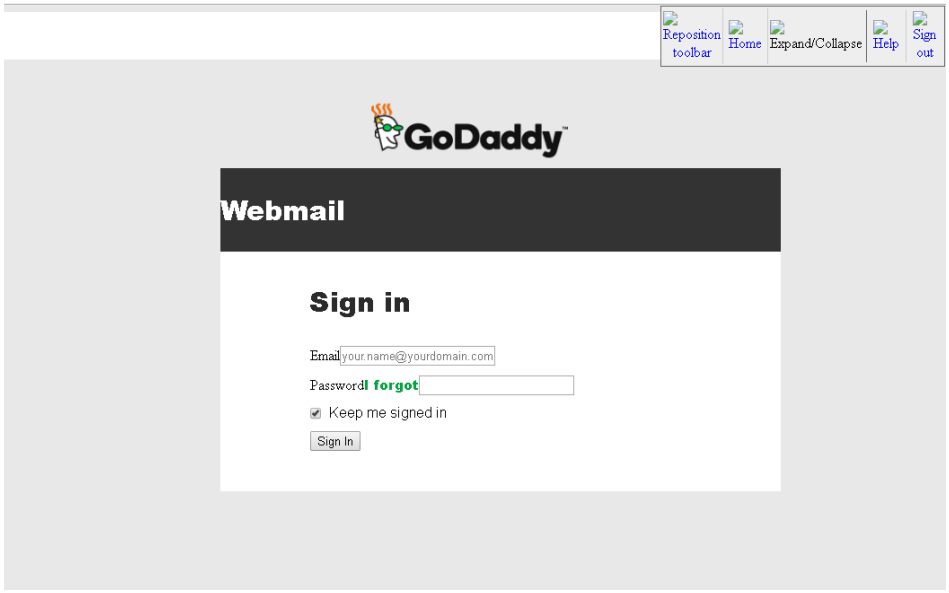

Fig. 4.2.16: Página de acceso al correo de empresa

Se aprecia que a pesar de acceder al correo, este no se muestra correctamente. Por lo tanto, se debe modificar el acceso web creado para que Pulse Secure redirija y cargue correctamente el correo.

Una vez estudiado el caso y el motivo por el cuál no se cargaba como debía, vemos que hacía falta habilitar otra política más. Se configura la política de *Rewriting* seleccionando la opción de *No rewriting*.

Tras dicha modificación, volvemos a probar el enlace y el resultado obtenido es el siguiente.

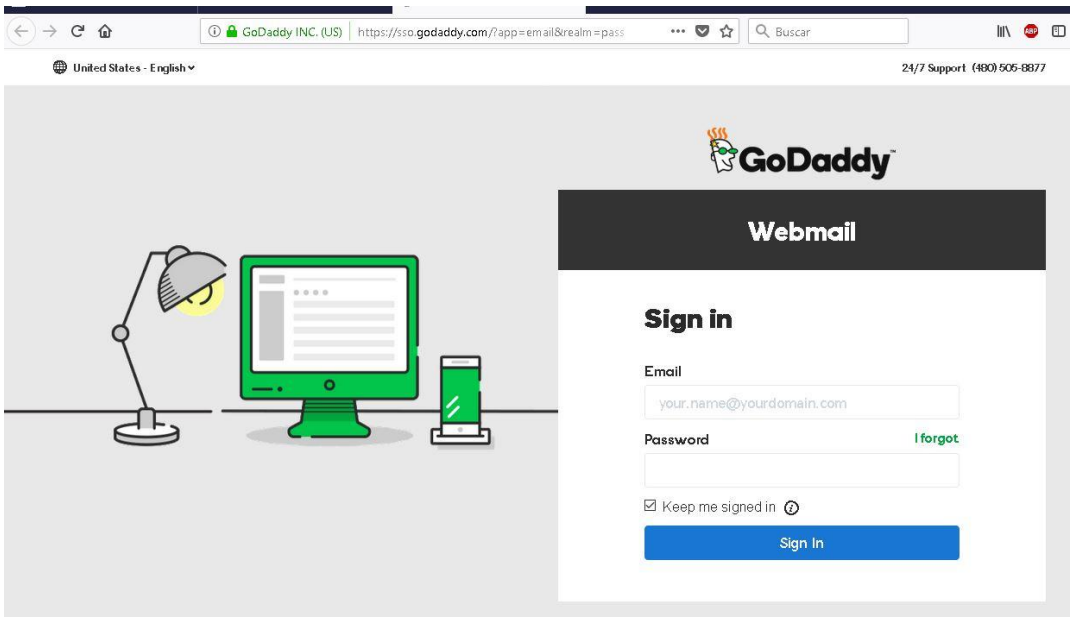

Fig. 4.2.17: Acceso correcto al correo de empresa

2. Terminal Services

Para el caso del *Terminal Services*, se va a crear un acceso al escritorio remoto donde la empresa tiene guardada una hemeroteca propia que utilizan los trabajadores para la creación de sus respectivos artículos. Al encontrarse en otra red, se va a crear un *Terminal Services* del tipo Windows Terminal Services, el cual va a estar asignado al rol correspondiente al grupo de usuarios Analytics, Role_Analytics.

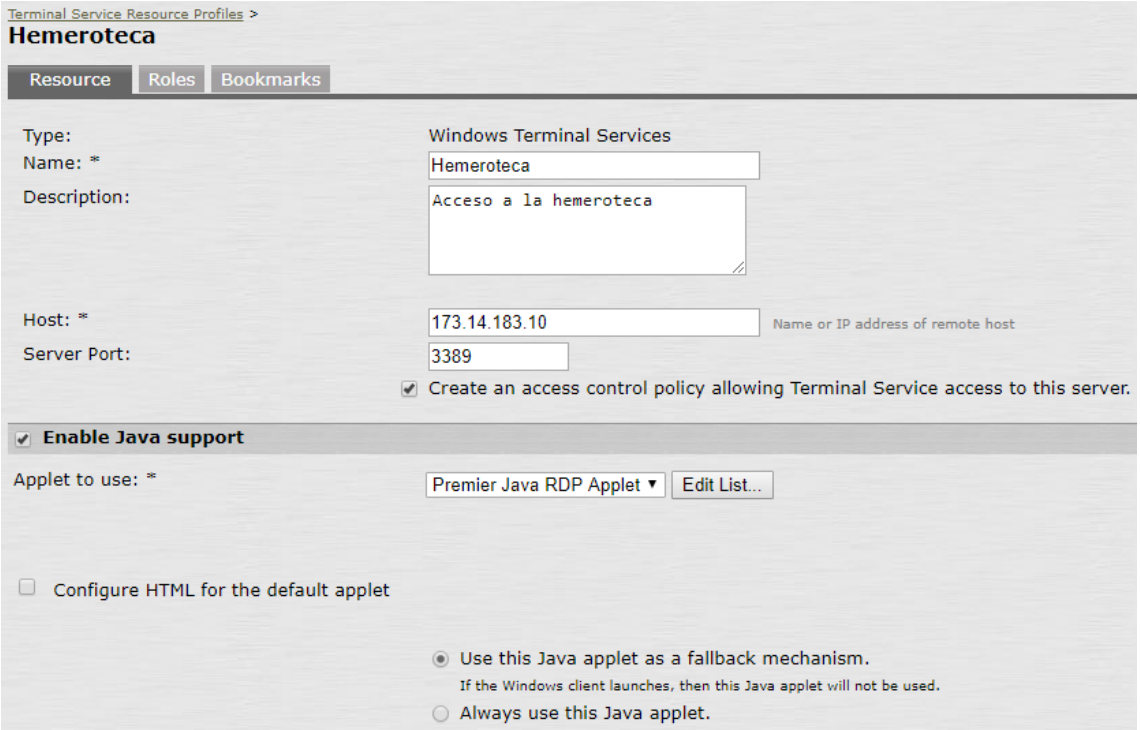

Fig. 4.2.18: Creación del acceso a la hemeroteca

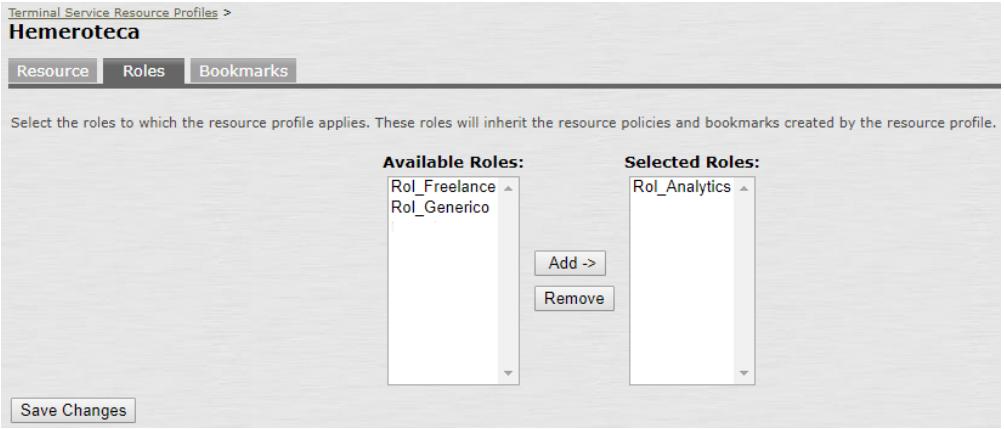

Fig. 4.2.19: Asignación del acceso a Analytics

Fig. 4.2.20: Creación del bookmark de hemeroteca

En cuanto los usuarios que pertenezcan a Analytics accedan al portal verá los accesos al correo, creado anteriormente, y a la Hemeroteca.

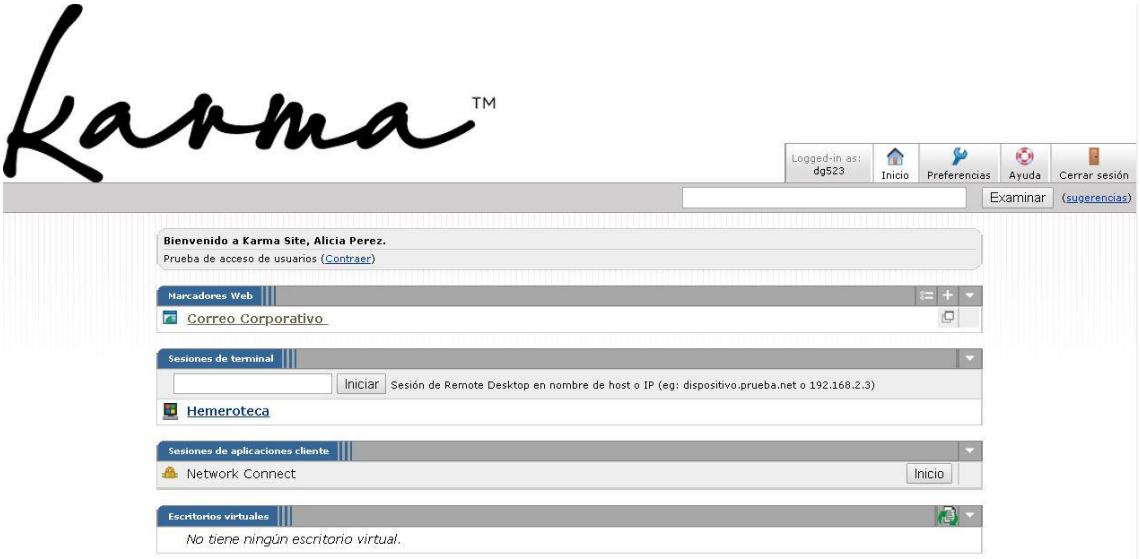

Fig. 4.2.21: Página de inicio de un usuario del grupo Analytics

3. Bookmark tipo web

Se va a configurar el acceso a la página de edición web para el blog que lleva la empresa.

Se creará un acceso web de tipo Custom en donde se va a introducir la url del sitio de edición web. Este enlace irá asociado al rol de los usuarios que pertenecen al grupo de Freelance, Rol_Freelance.

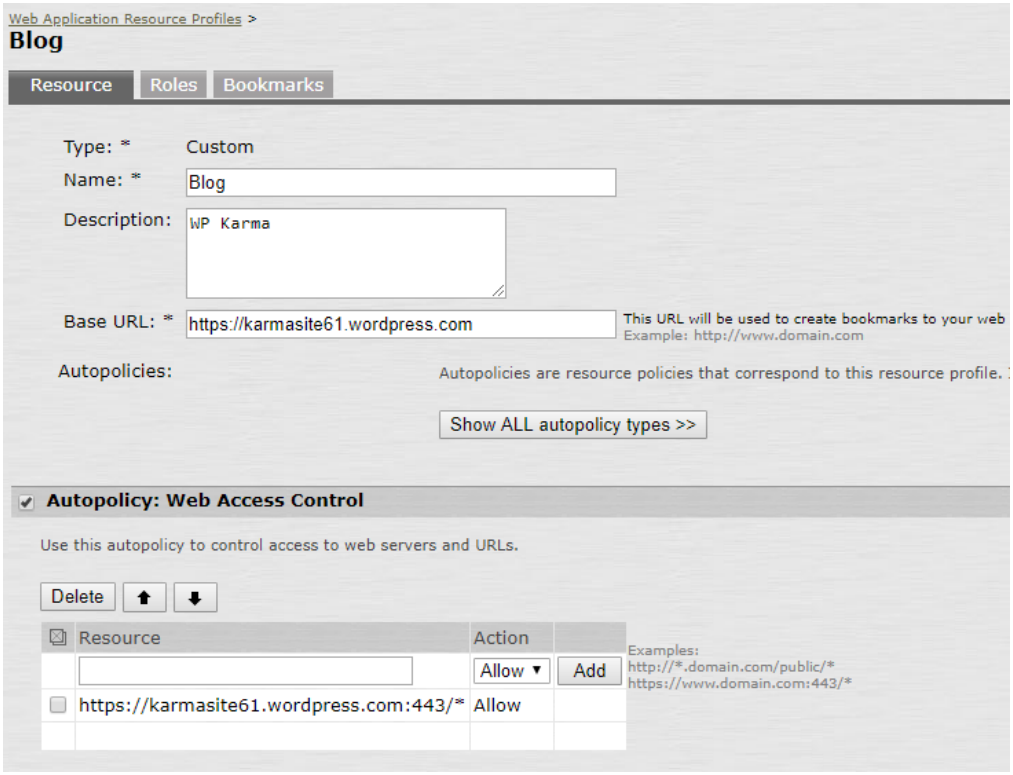

Fig. 4.2.22: Creación del enlace al blog

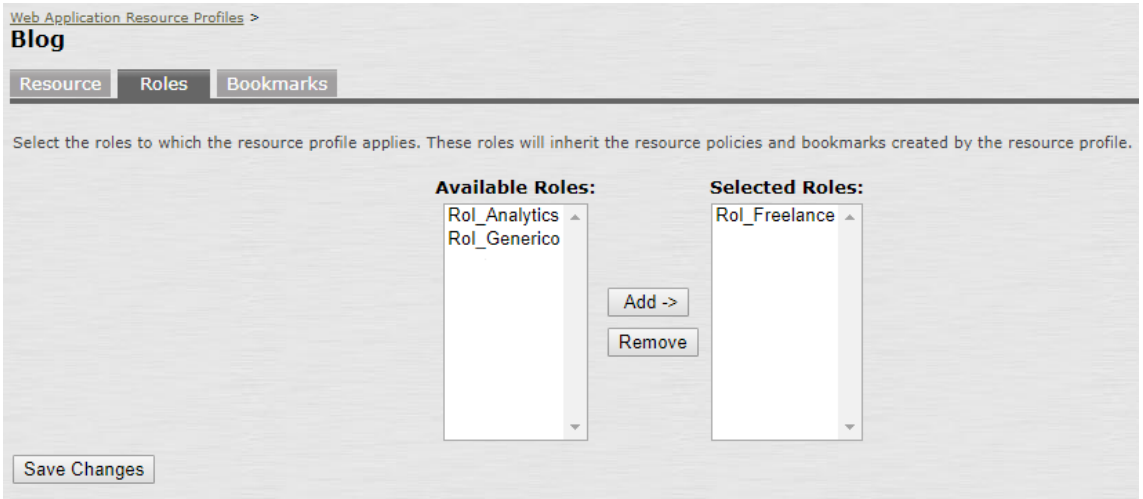

Fig. 4.2.23: Asignación del acceso a Freelance

Fig. 4.2.24: Creación del bookmark del blog

Al igual que ha pasado con el correo, en este caso el blog también se ve como texto plano.

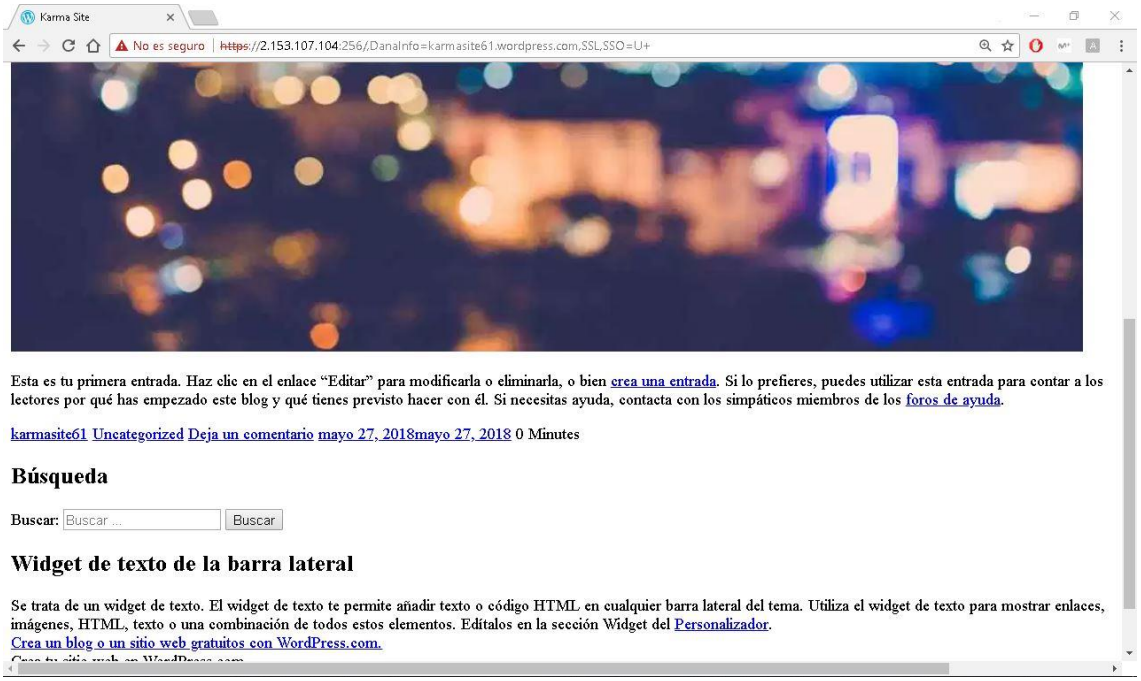

Fig. 4.2.25: Página de acceso al blog

Hay que tener en cuenta que el bookmark funciona como un proxy inverso, ARU internamente hace la petición al servidor web de la empresa y transcribe todo el código para que se reciba como HOST/servidor web la IP del ARU.

Por lo que esto puede ser debido a algún problema con la reescritura, en cuyo caso es necesario estudiarlo a fondo utilizando herramientas y analizadores para ir viendo paso a paso tanto lo que devuelve el servidor como lo que llega al ARU y lo que este reescribe hasta al navegador.

Se procede a realizar lo mismo que en el caso anterior, ya que los problemas de reescritura se suelen solucionar con la opción de Passthrough. Por lo tanto, se activa la política de *rewriting* con la siguiente opción.

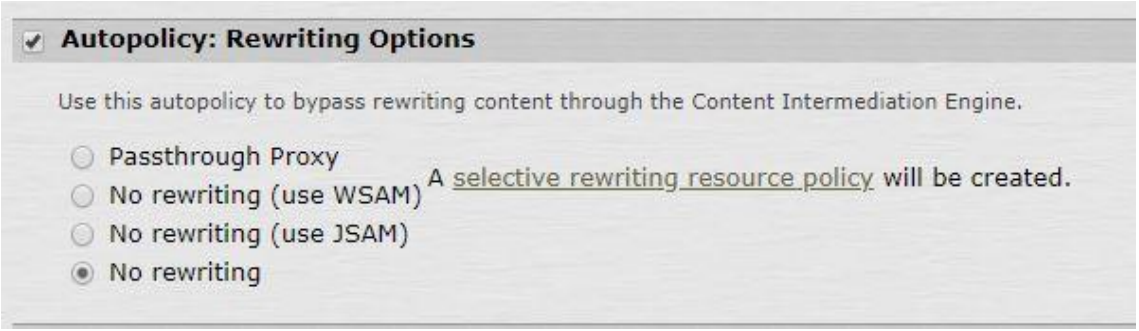

Fig. 4.2.26: Cambio realizado en la política de rewriting

Tras el cambio realizado, se vuelve a cargar el bookmark y vemos como ya aparece cargado correctamente el blog.

Fig. 4.2.27: Página correcta del blog

Finalmente se procede a configurar el apartado del Host Checker para cumplir con las especificaciones de seguridad dadas por la empresa.

Primero, se crea una política que indique que el sistema operativo del ordenador desde donde se va a acceder sea Windows 7 con SP1. Para esto se crea una nueva regla del tipo 'OS Checks'.

Segundo, se crea una política que compruebe el antivirus del ordenador desde donde se va a acceder. En este caso, debe haber pasado el antivirus hace dos días o menos, en caso de no cumplirlo, se lanzará un escaneo en el momento y cuando se obtenga como resultado que no hay amenazas, dejará acceder al usuario.

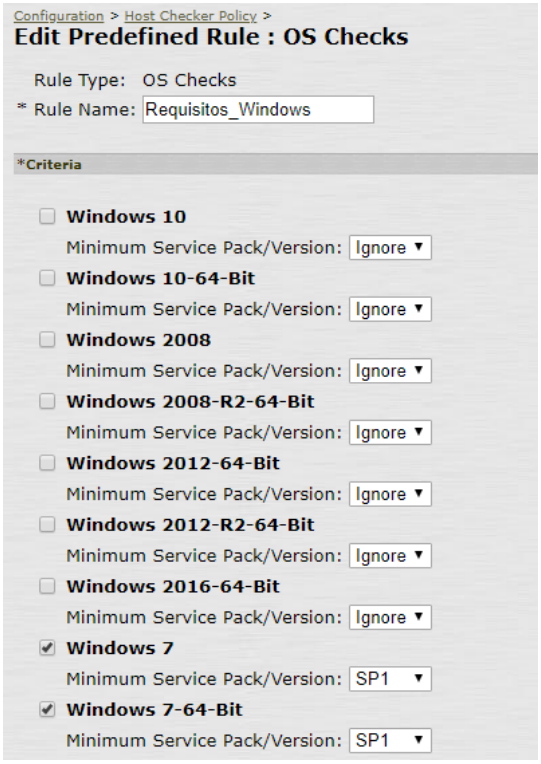

Fig. 4.2.28: Regla Sistema Operativo obligatorio

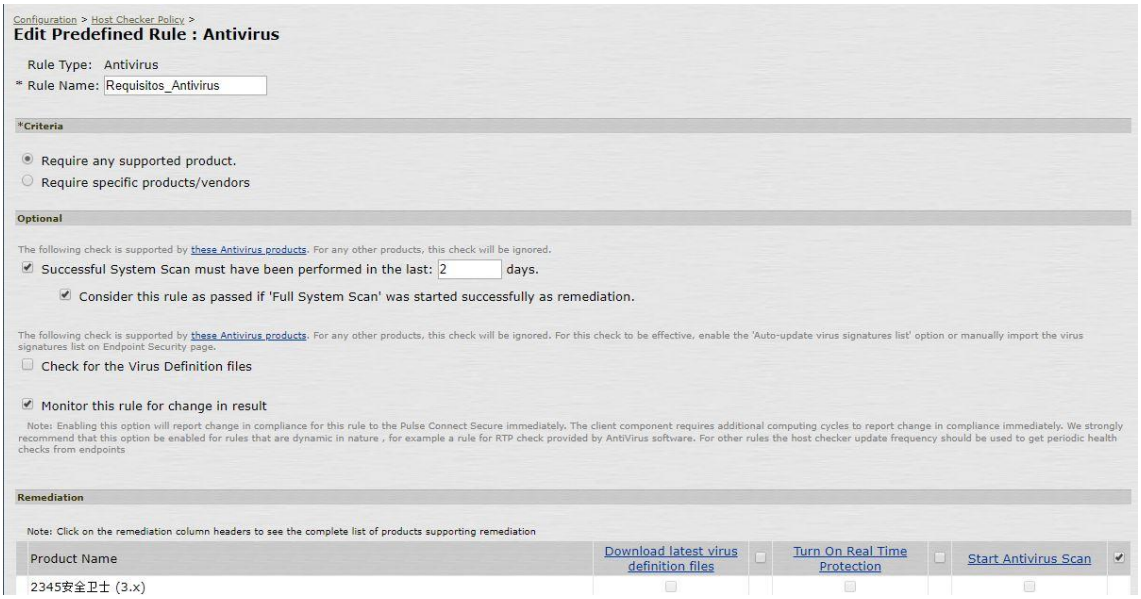

Fig. 4.2.29: Regla Antivirus obligatorio

Al finalizar la configuración de estas dos políticas, obtendremos un cuadro resumen de nuestro Host Checker.

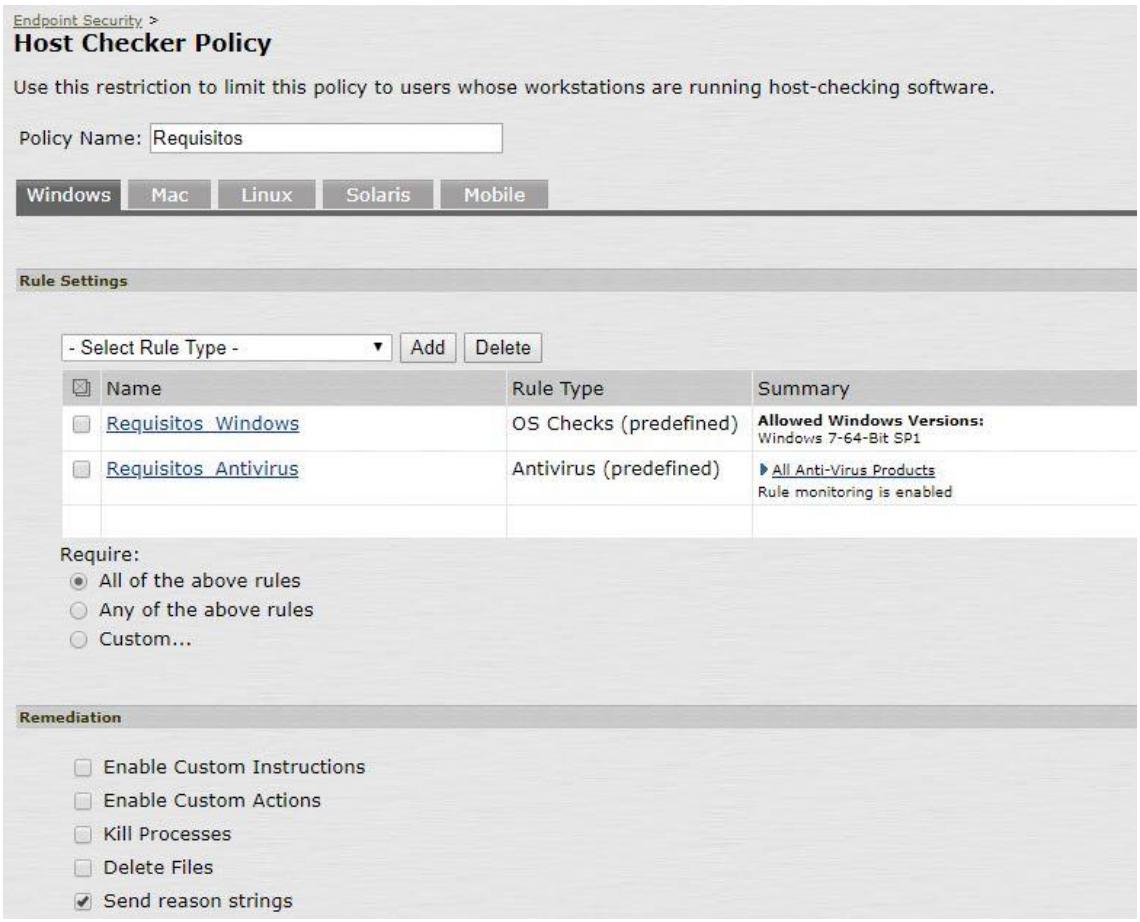

Fig. 4.2.30: Resumen de los requisitos del Host checker

Por último, se accede a todos los roles que quieran que cumplan estas reglas y se les activa el Host Checker. En nuestro caso, se requiere que todos los usuarios pasen dicho test.

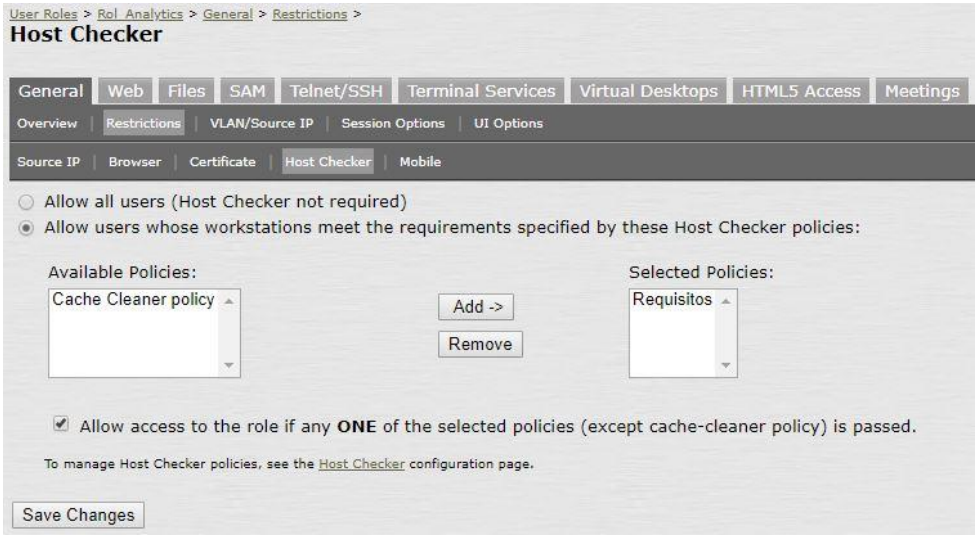

Fig. 4.2.31: Activación del Host checker en los roles

4.3 Escenario 2. Caso complejo de acceso a recursos externos

Una empresa ha decidido unificar todas sus herramientas en una y ha optado por integrar ARU en su red.

Al partir de un entorno que el cliente ya tenía montado, hay que tener cuidado al adaptarlo a ARU, pues los métodos de acceso y las configuraciones previas pueden no ser lo más óptimo a la hora de unificarlo con este nuevo entorno. Pero sabemos que ARU dispone de diferentes combinaciones para poder adaptarse de la mejor forma posible.

Esta empresa dispone de un directorio activo en donde se encuentran todos sus empleados. También tienen creados diferentes grupos de usuarios diferenciados por su puesto de trabajo, y en donde tienen diferentes permisos de acceso a recursos según las necesidades de cada puesto.

Lo que más les urge es poder acceder a su ordenador de la oficina para poder trabajar en remoto, pues al estar realizando cambios en su entorno tienen que asegurarse que van a poder acceder a todos los programas y documentación que tienen allí, hasta que finalice todo el cambio. Con este cambio se obtendrá menos repercusión y será transparente para los trabajadores.

Por último, todos los usuarios deben poder acceder al correo de la empresa, que en este caso es Office 365. Esto junto con lo anterior son los puntos fuertes a cumplir en esta primera fase.

Resumiendo, las condiciones a cumplir son:

- El acceso de los usuarios va a través del directorio activo.
- Habilitar acceso a Office 365.
- Habilitar VPN Tunneling

Se va a comenzar por crear la configuración del directorio activo para que los usuarios puedan acceder con dichas credenciales, aumentando la seguridad de inicio de sesión, ya que se evita el acceso a personal no autorizado.

Al tratarse de usuarios de directorio, los usuarios se cargan automáticamente cuando inician sesión en el portal de acceso de usuarios, pues utilizan las mismas credenciales y tiene los mismos permisos de accesos a recursos que tienen en el directorio de la empresa. Por ello sólo se necesita configurar el vínculo entre el DA y la herramienta en la pestaña de *Settings*.

Fig. 4.3.1: Configuración DA de la empresa

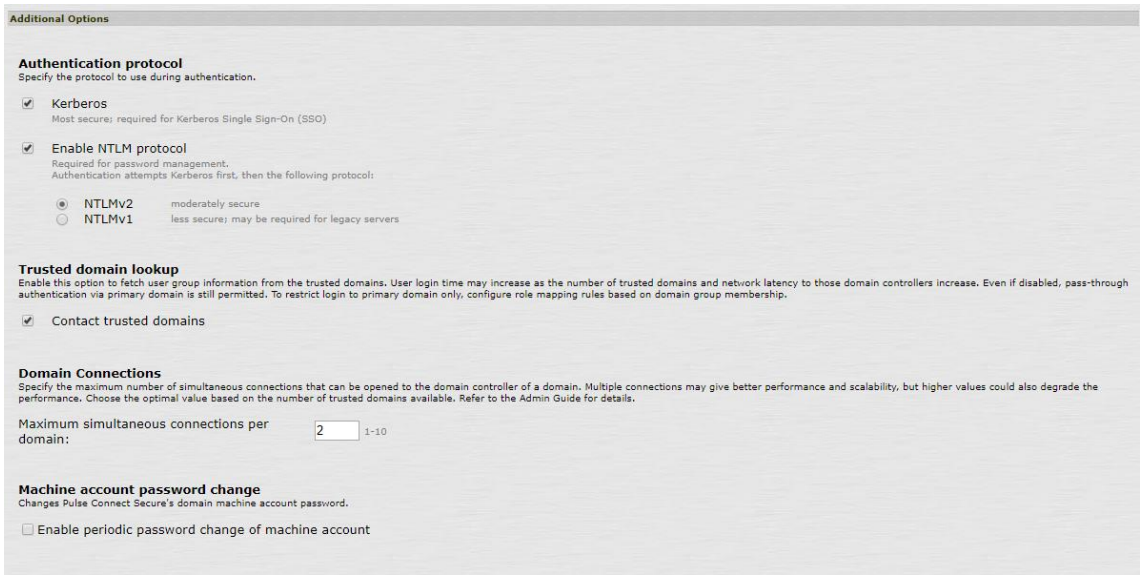

Fig. 4.3.2: Configuración DA de la empresa

Una vez creado el directorio, se le va asignar un Realm y un Rol. Estos se asignarán a los usuarios del DA y con ello se podrán realizar mapeos para dar o no permisos a los diferentes recursos a configurar.

Primero se crea el Rol, para indicar a qué recursos van a tener acceso los usuarios que se les asignen este rol. En este caso, se habilita el acceso Web y el VPN Tunneling.

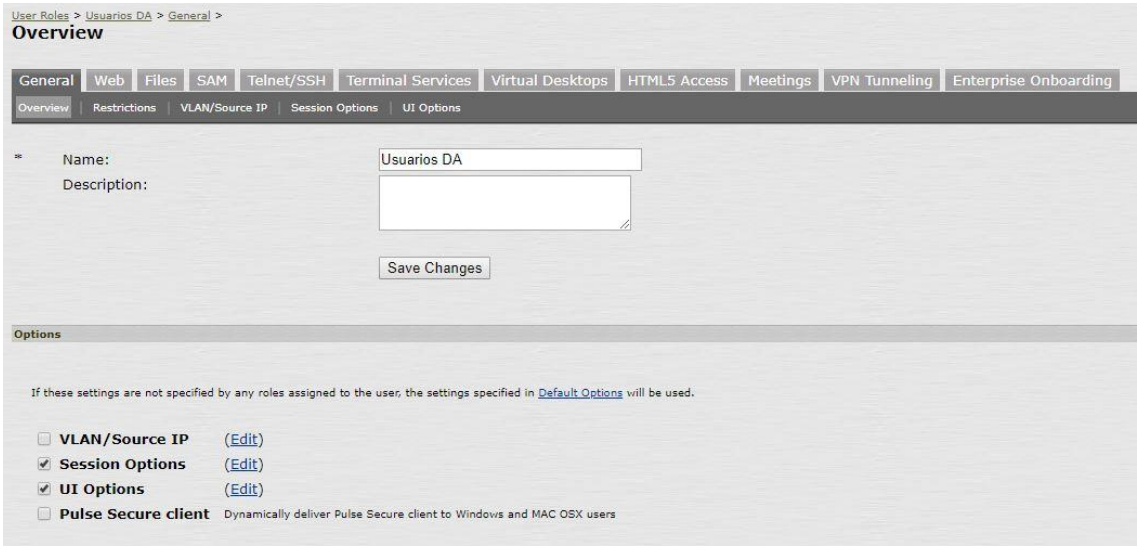

Fig. 4.3.3: Creación del Rol

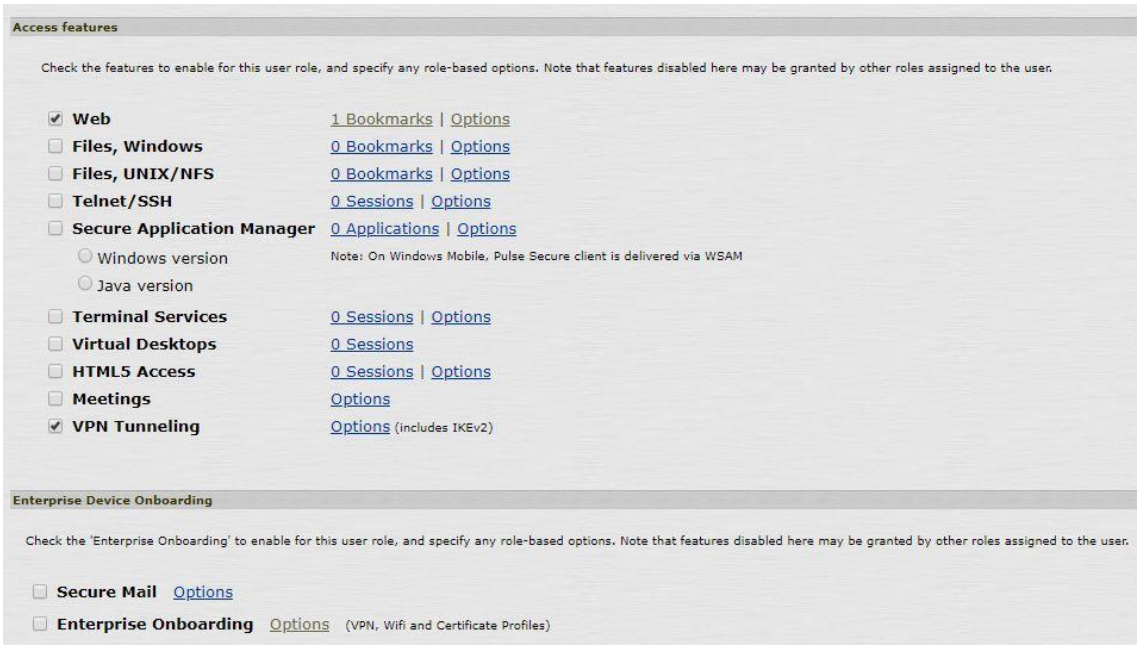

Fig. 4.3.4: Creación del Rol

A continuación se crea el Realm. Como se observa en la siguiente figura, en *Authentication* se selecciona el directorio activo. Así se aplicará este Realm a los usuarios que pertenezcan a ese DA. Esto junto con el *Role Mapping* que se muestra en la figura 4.3.7, se consigue que al autenticarse un usuario se le asigne uno u otro Rol dependiendo del mapeo realizado. En este caso, en el mapping se ha puesto como regla una genérica (*), esto quiere decir que todos los usuarios que pertenecen al DA se les va a asignar el rol creado anteriormente.

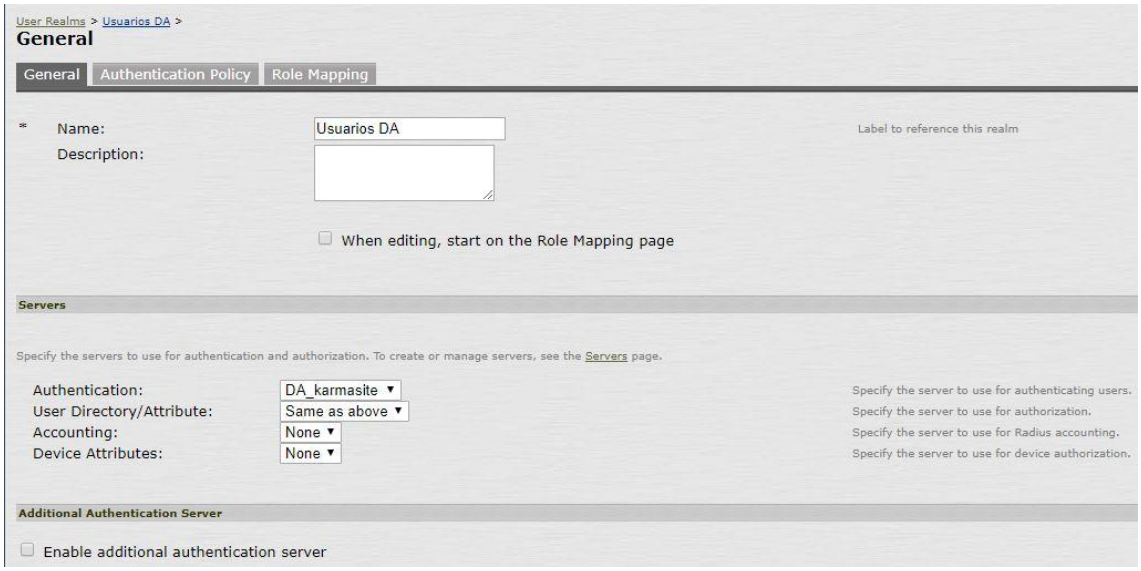

Fig. 4.3.5: Creación del Realm

Fig. 4.3.6: Creación del Realm

Fig. 4.3.7: Creación del Role Mapping

Una vez que se tiene configurado los accesos, se procede con la creación de los diferentes recursos. En este caso son:

1. Correo Office 365
2. VPN Tunneling

1. Correo Office 365

Para el caso de Office 365, observamos que no existe ningún bookmark de tipo O365, sino que todos son Microsoft OWA. Es importante tener presente que O365 no se comporta igual que el correo Exchange, pues este agrupa diferentes herramientas de Microsoft y se facilita el acceso mediante web a Word, Excel, Sharepoint, Correo…Por este motivo, realizar esta configuración en ARU no es sencillo. [34]

Realizar esta integración implica tener que realizar un estudio de cómo se comporta O365, que peticiones hace, de que tipo son, que enrutamiento realiza, etc. Todo esto es importante conocerlo, pues la solución o soluciones aportadas van a depender de ello y el resultado tiene que ser perfecto, es decir, el usuario debe ver y utilizar la herramienta O365 igual que si no estuviera a través de ARU. Por ello se deben soportar todas las funcionalidades, pues no vamos a saber lo que va a utilizar cada usuario.

Partiendo de este escenario, primero se va a probar con la configuración estándar de un bookmark y se va a comprobar el resultado.

Se crea un bookmark del tipo *Custom* y se asigna al rol que incluye a todos los usuarios del directorio. Tal y como se observa en la figura, se habilita el control de acceso, el cual se ha creado automáticamente.

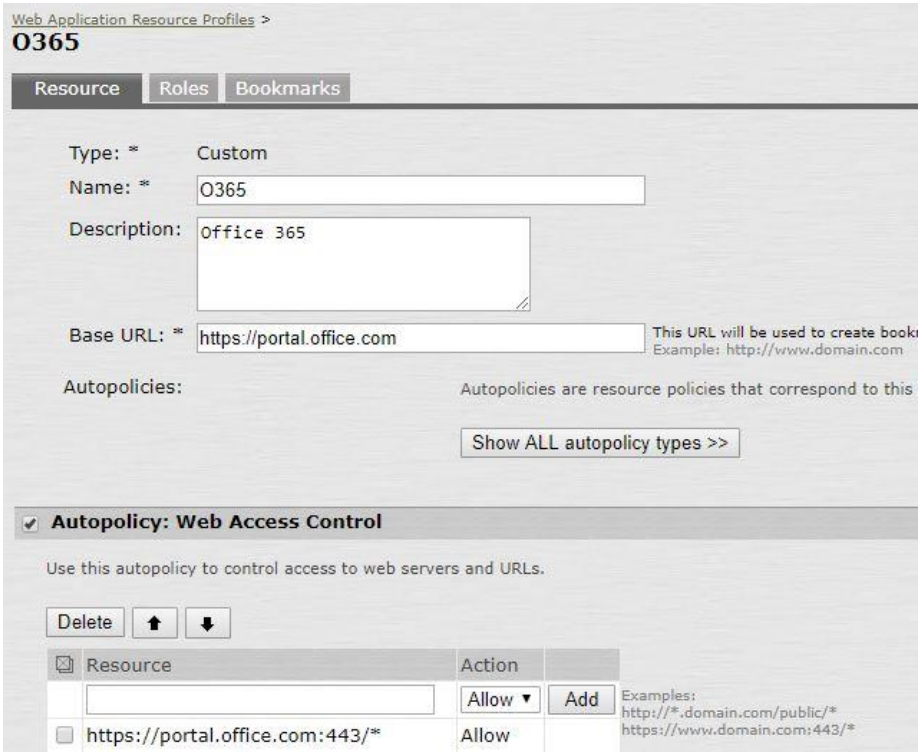

Fig. 4.3.8: Configuración acceso a Office 365

Con esta configuración no se accede al correo. Pues aparece el siguiente mensaje.

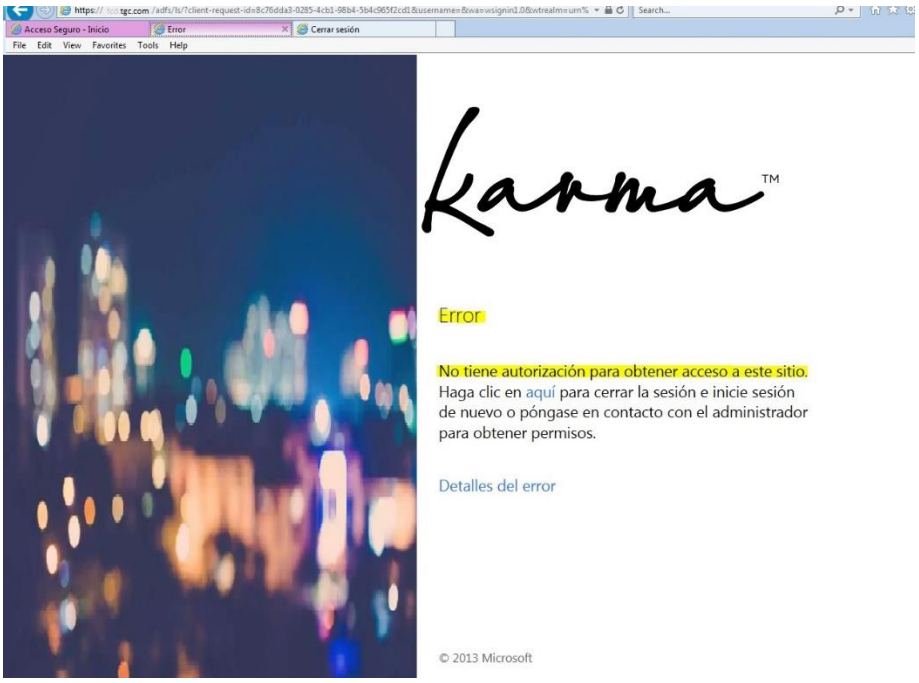

Fig. 4.3.9: Acceso denegado a través de IP pública

Esto se debe a que está restringido el acceso desde fuera con una IP pública, por eso es importante que el tráfico salga por la sede central de la empresa, ya que ahí sí está permitida esta IP.

Otro punto a tener en cuenta es que no hay acceso a la IP privada del dominio de la empresa. Para ello, se configura un host para que redireccione a la IP pública.

Fig. 4.3.10: Configuración del host

A continuación se agregan en el bookmark una serie de urls de redireccionamientos internos para comprobar si se accede o no al correo.

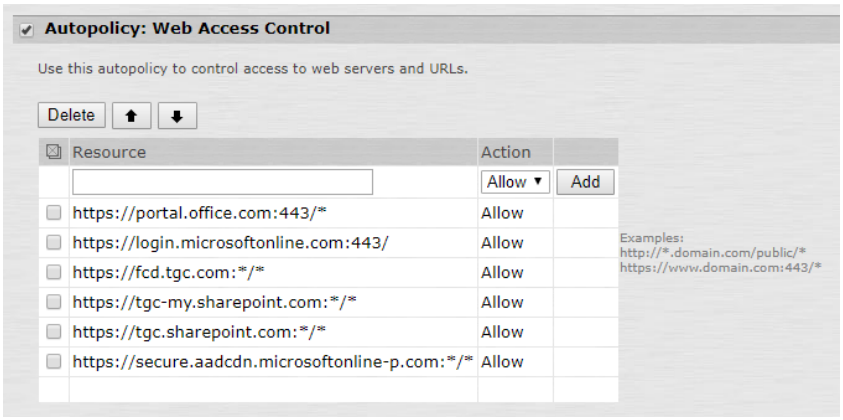

Fig. 4.3.11: Cambios realizados en la política

El resultado que se obtiene ahora es mejor que el anterior, pue ya podemos acceder, pero no se visualiza correctamente el correo. Lo que se ve cuando se accede es lo siguiente:

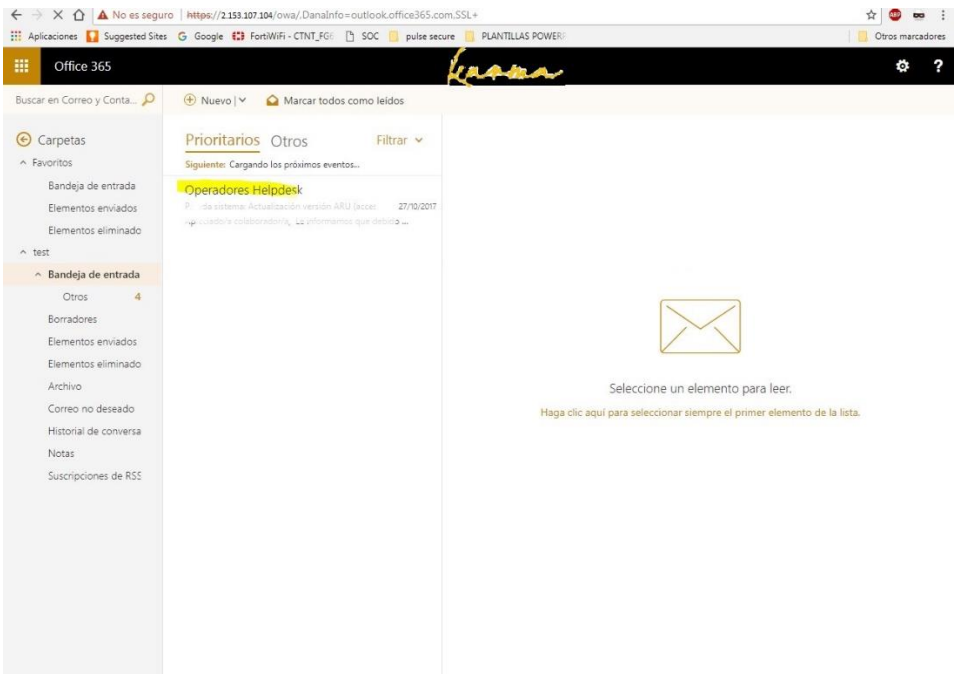

Fig. 4.3.12: Error al visualizar el correo en la parte de la derecha

Como hemos podido observar, aunque se acceda a Office 365, no reconoce que hay seleccionado un correo para previsualizar y el menú tampoco carga completamente.

Para poder entender mejor que sucede, se abren las opciones de desarrollador y se observan las siguientes trazas.

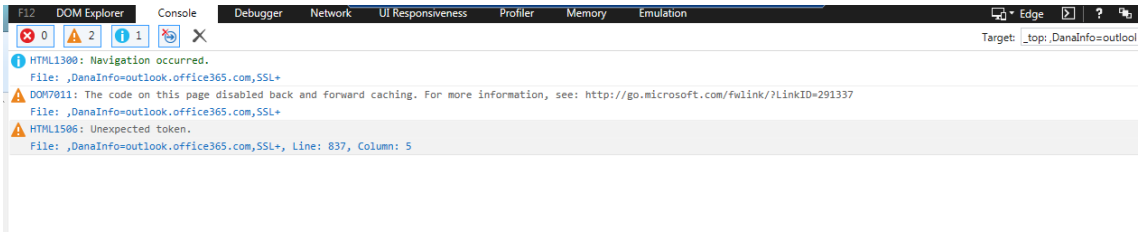

Fig. 4.3.13: Trazas obtenidas con la opción de desarrollador

Ayudándonos de la web de Microsoft que nos indican, podemos ver que la parte del menú está realizado en typescript por opensource. A pesar de saber que está ocurriendo, no se puede modificar dicho comportamiento con las opciones disponibles del bookmark, por eso se descarta esta opción. Por consiguiente, se realiza una tercera prueba.

En este caso, se va a realizar una configuración con WSAM (*Windows Secure Application Manager*). Antes de comenzar con el despliegue de esta herramienta, se va a explicar brevemente en que consiste WSAM. [30] [35] [36]

La opción Secure Application Manager (SAM) proporciona un acceso remoto seguro a nivel de aplicación a servidores empresariales desde aplicaciones cliente. Puede implementar dos versiones:

- WSAM: La versión de Windows es una solución basada en Windows que le permite proteger el tráfico a aplicaciones cliente/servidor individuales y servidores de aplicaciones.
- JSAM: La versión de Java brinda soporte para aplicaciones cliente/servidor de TCP estático, incluido soporte mejorado para Microsoft MAPI, Lotus Notes y Citrix NFuse. JSAM también proporciona soporte NetBIOS, que permite a los usuarios asignar unidades a recursos protegidos específicos.

Tras conocer en qué consiste WSAM, vemos que se puede adaptar a lo que necesitamos. Se procede a realizar la configuración para posteriormente realizar pruebas de acceso al correo y estudiar el resultado.

Primero se configura un nuevo role ‘WSAM_O365’ habilitando la opción de WSAM para su posterior configuración.

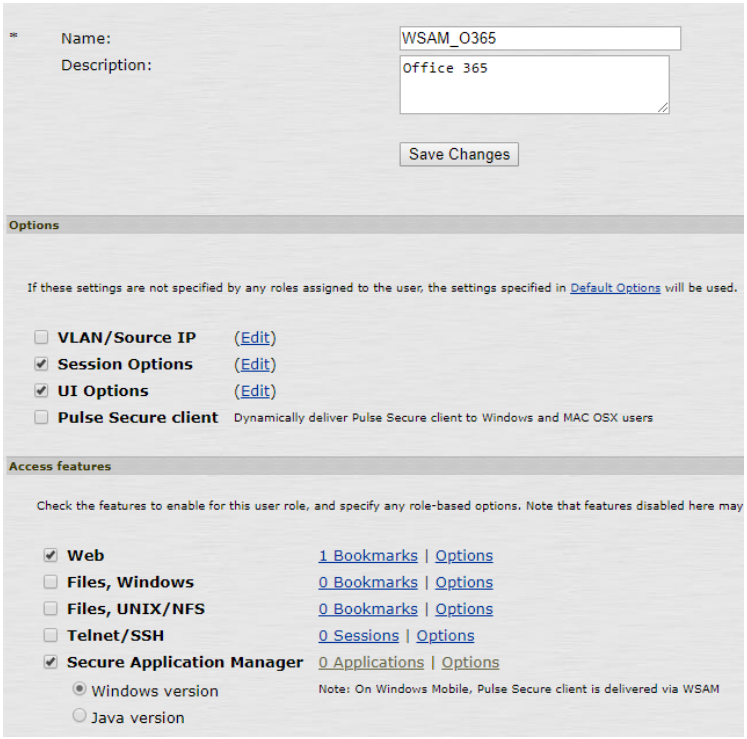

Fig. 4.3.14: Activación de la opción de WSAM

Al disponer de rol al que asignar esta implementación, se realiza el WSAM. Aquí se agregarán todas las urls que intervienen tanto explícita como implícitamente.

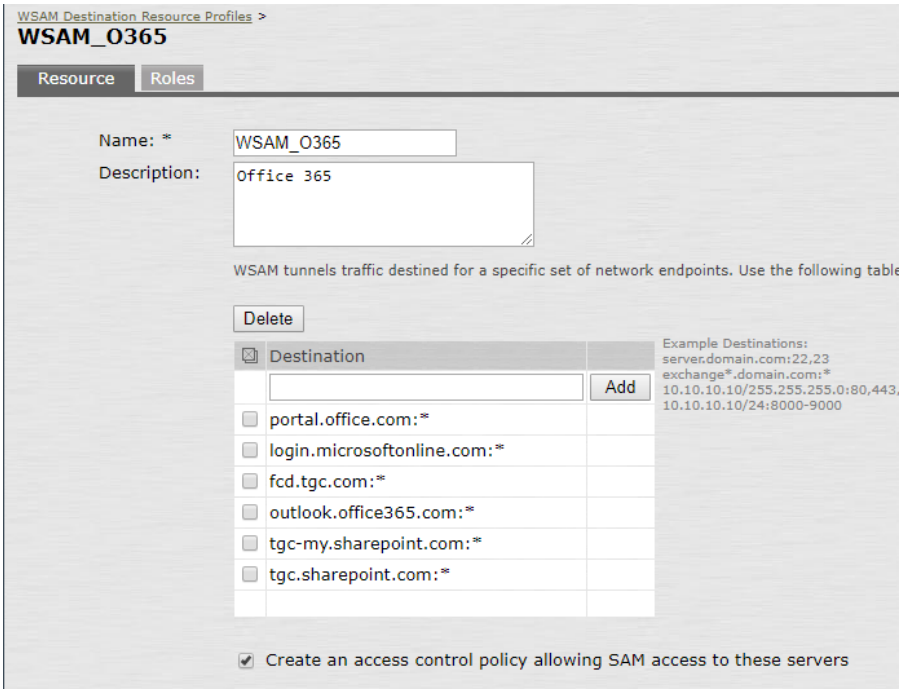

Fig. 4.3.15: Configuración de WSAM

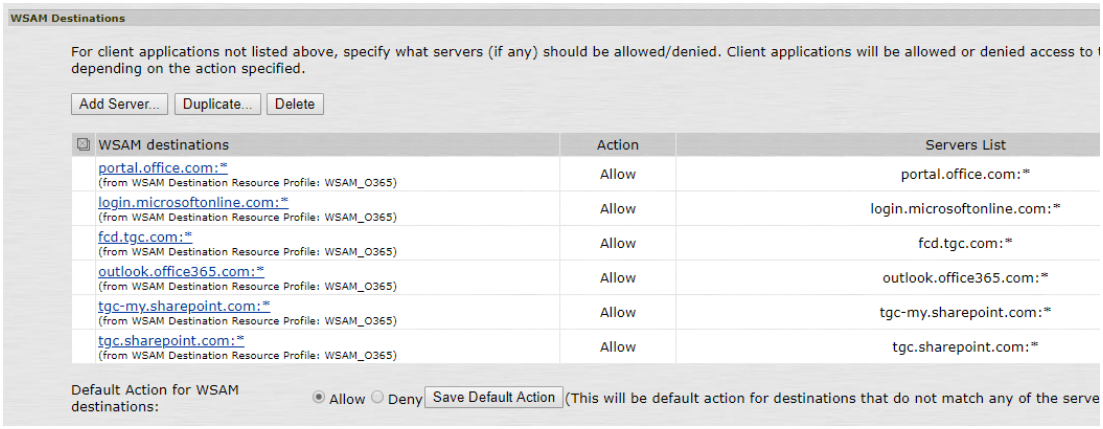

Fig. 4.3.16: Destinos permitidos a través de WSAM

Una vez finalizada la implementación con WSAM, debemos asignar el bookmark creado anteriormente al mismo rol que este, 'WSAM_O365'. Ya que debemos disponer del enlace al correo una vez se establezca la comunicación a través de WSAM.

Para ello, nos logamos con un usuario de directorio y vemos los siguientes enlaces.

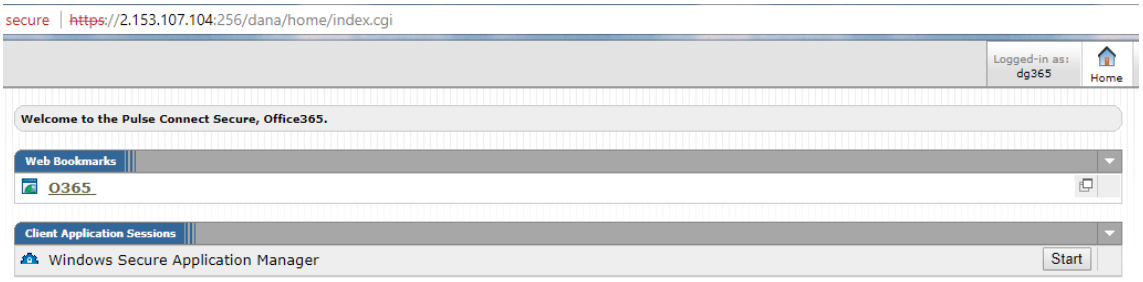

Fig. 4.3.17: Accesos disponibles tras acceder con un usuario de DA

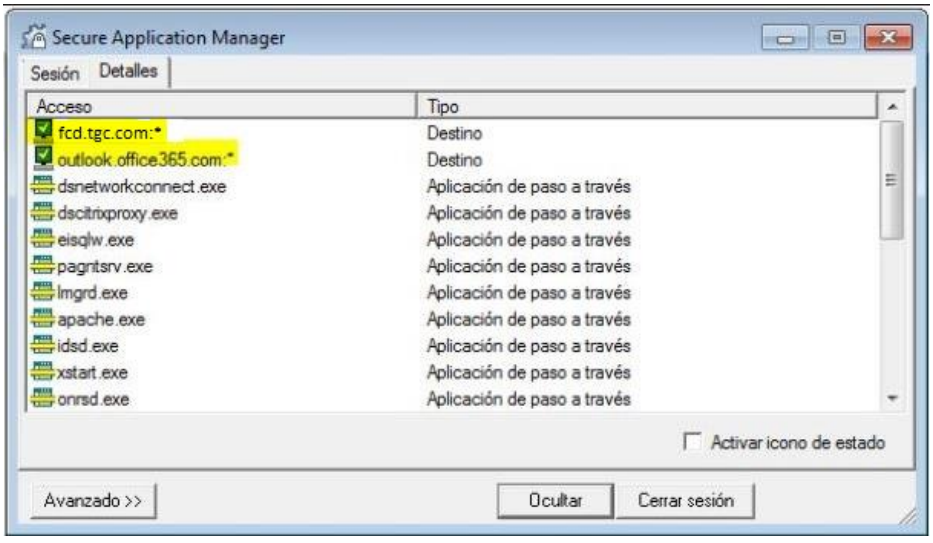

Fig. 4.3.18: Rutas de accesos con WSAM

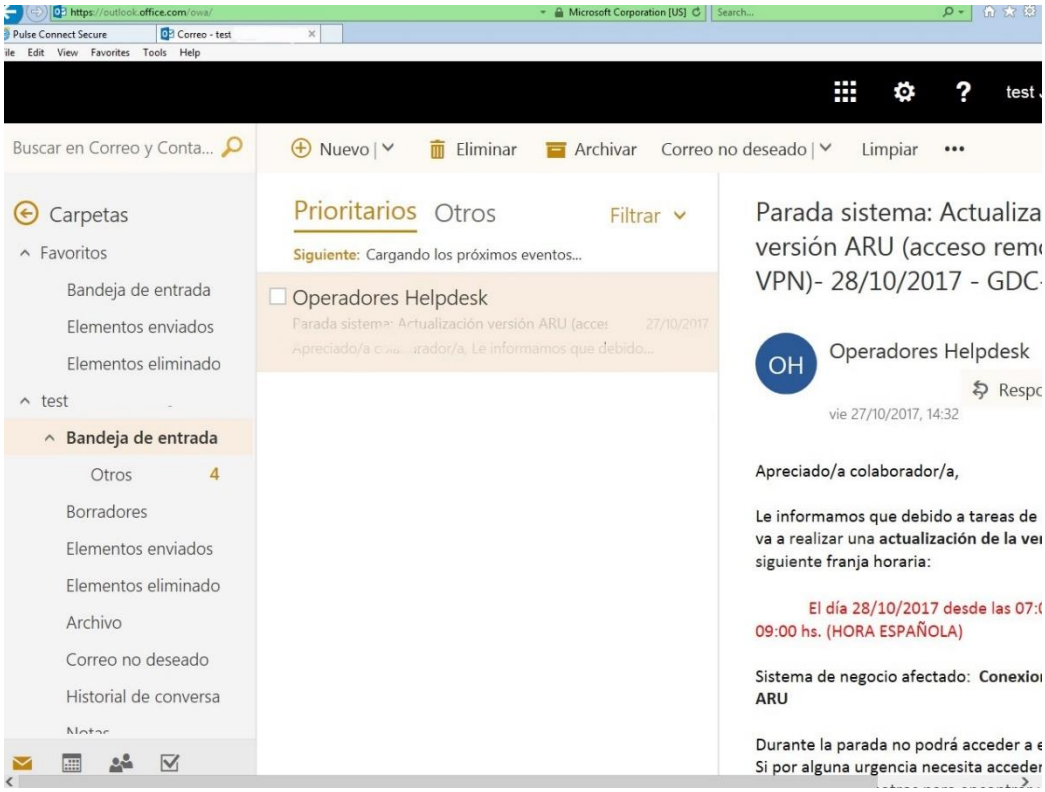

Fig. 4.3.19: Correo Office 365

Finalmente, tras realizar una combinación del bookmark para Office 365 y la implementación de WSAM, se ha podido acceder correctamente al correo y visualizar todos los campos correctamente.

2. VPN Tunneling

VPN Tunneling permite a los usuarios conectarse en remoto a la red de la oficina, asignándole una IP del rango establecido y dedicado para este fin. Dicha asignación se puede realizar directamente a una persona o a un departamento, para que tengan siempre la misma IP o el mismo rango de IPs respectivamente.

Para que el usuario pueda conectarse en remoto, se debe descargar en su ordenador el cliente de Pulse Secure [37]. Dicho agente aparece en la página de inicio a la que accede el usuario para ver sus recursos. Una vez descargado no es necesario volverlo hacer, pues se queda instalado en el ordenador y se puede iniciar la conexión en remoto abriendo directamente el agente pesado, introduciendo la IP pública y las credenciales correspondientes.

Después de explicar en qué consiste VPN Tunneling, se va a realizar la configuración para habilitar los accesos.

Lo primero, es tener definido el rango que se va a destinar a este uso dependiendo del número de conexiones concurrentes se vayan a tener. En este caso, se han habilitado desde la .100 hasta la .170 de la red de la empresa.

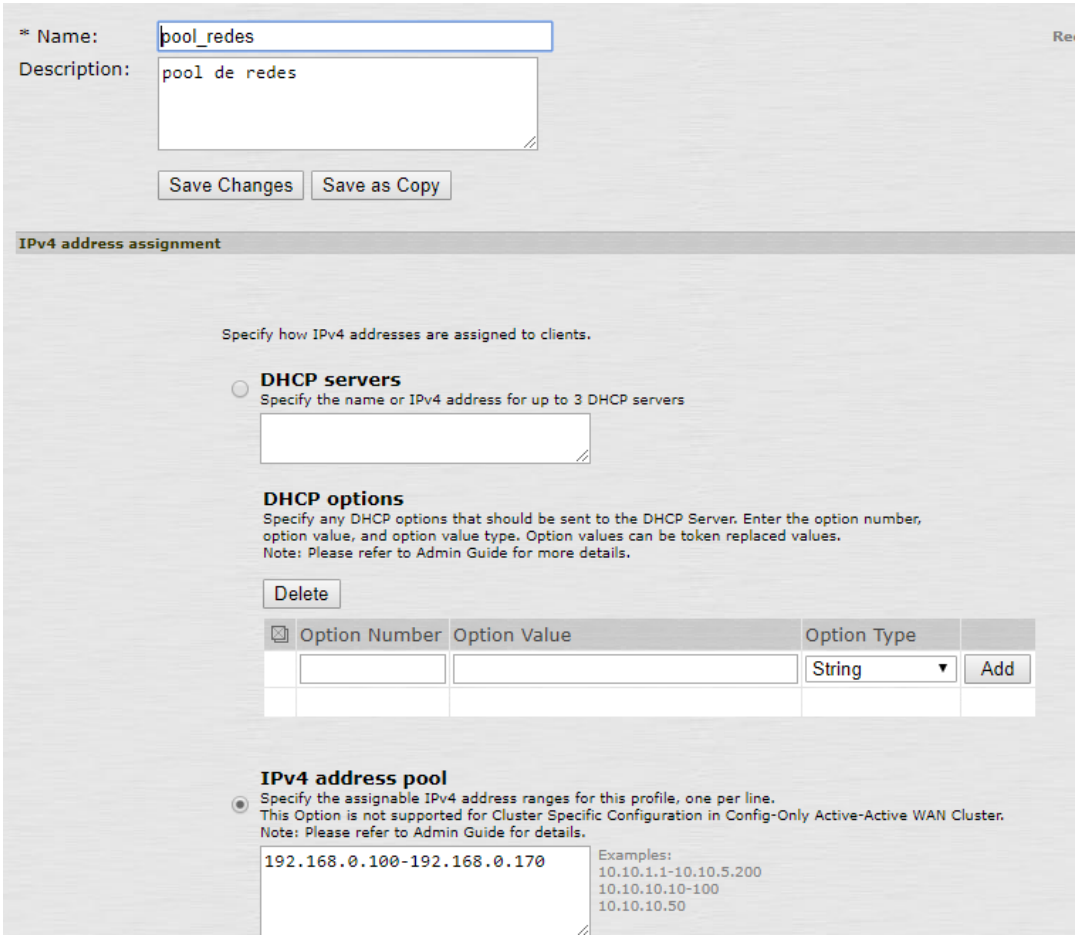

Fig. 4.3.20: Configuración del pool de redes

Se habilita el control de acceso, en caso de dejar el acceso sin restricción se pondrá un *.

Fig. 4.3.21: Configuración del control de acceso

Para finalizar, se configura el Split Tunneling para que todo el tráfico perteneciente a esos intervalos vaya por el túnel. Una vez creado, hay que habilitarlo en el rol correspondiente. Esta configuración no es obligatoria y depende de las necesidades de la empresa.

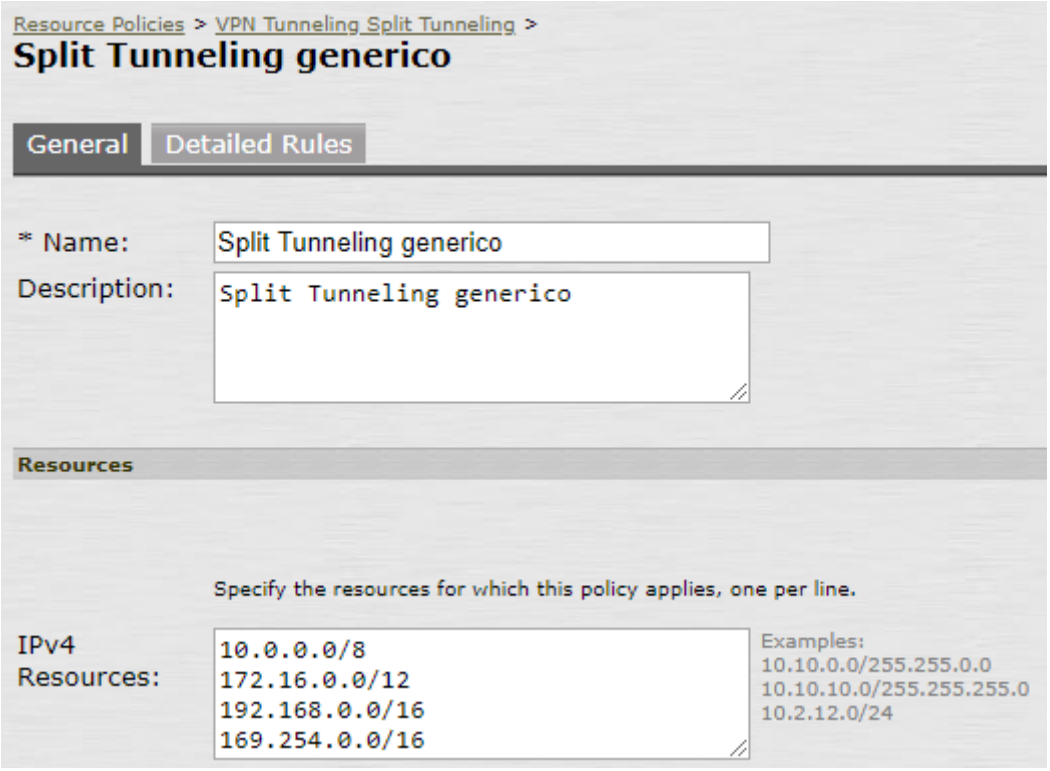

Fig. 4.3.22: Configuración del Split Tunneling

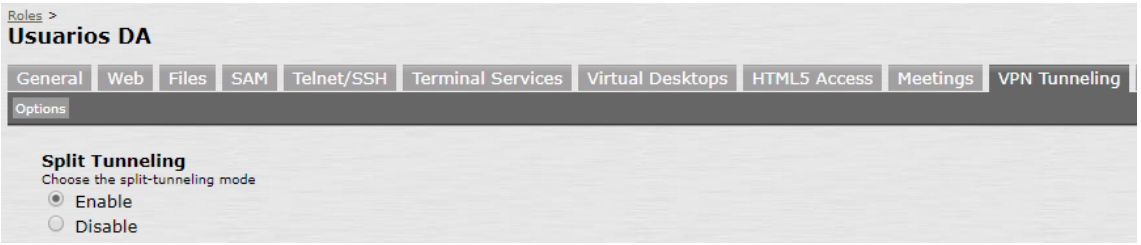

Fig. 4.3.23: Habilitar Split Tunneling en el Rol

Una vez finalizado todo el proceso, nos descargamos el agente pesado y realizamos la conexión desde ahí de la siguiente forma.

Fig. 4.3.24: Conexión con el agente pesado de Pulse Secure para VPN

4.4 Escenario 3. Caso complejo de autenticaciones

En este escenario se van a tratar algunos de los tipos de doble factor de autenticación (2FA) que ofrece ARU. Para estos casos no es necesario que siempre los usuarios sean de directorio, sino que cada configuración se corresponderá con un tipo de integración.

Estas opciones son bastante solicitadas por empresas, pues facilitan los accesos y las autenticaciones a los usuarios sin disminuir la seguridad al respecto.

Tener en cuenta que todas estas integraciones se pueden combinar con las configuraciones vistas en los escenarios anteriores, pudiendo tener el acceso a la empresa más o menos restrictivo.

1. 2FA integrado con SAML

SAML (*Security Assertion Markup Language*) [30] [38] es un estándar que define un esquema XML para comunicar autenticación de usuarios, derechos e información de atributos. El estándar define las confirmaciones basadas en XML, protocolos, enlaces y perfiles utilizados en la comunicación entre entidades de SAML. SAML se usa principalmente para implementar el SSO (*Single Sign-On*) y permite a las empresas aprovechar el sistema de seguridad basado en

identidad como Pulse Connect Secure para hacer cumplir el acceso seguro a sitios web y otros recursos sin que el usuario tenga más de una solicitud de autenticación.

Cuando se implementa, Pulse Connect Secure ejecuta un servidor SAML local que depende de la autenticación del proveedor de identidades SAML y de las aserciones de atributos cuando los usuarios intentan iniciar sesión. Una vez autenticado, los límites de acceso al sistema y a los recursos protegidos los impone la empresa.

Tras esta breve introducción a SAML se va a comenzar a realizar la integración en Pulse Secure. Para ello, es imprescindible disponer de la url que facilita el SAML de la empresa por la cual se establece la comunicación para validar el inicio de sesión único (SSO). Sin ella el sistema no redirigirá correctamente la solicitud del usuario y se le denegará el acceso. En este caso como se dispone del archivo de metadatos en formato xml, se carga directamente en la plataforma, generando automáticamente las urls para el SSO.

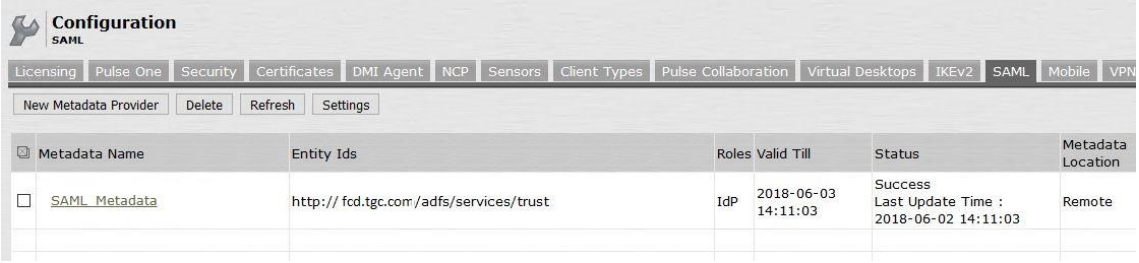

Fig. 4.4.1: Carga archivo Metadata para SSO

Una vez cargado el archivo, se continúa configurando el nuevo servidor de autenticación, que en este caso como cabe de esperar, será de tipo SAML. Se observa en la configuración que las urls aparecen cargadas automáticamente, pues tras subir el archivo de metadatos del servidor de SAML, se han creado las relaciones de confianza pertinentes.

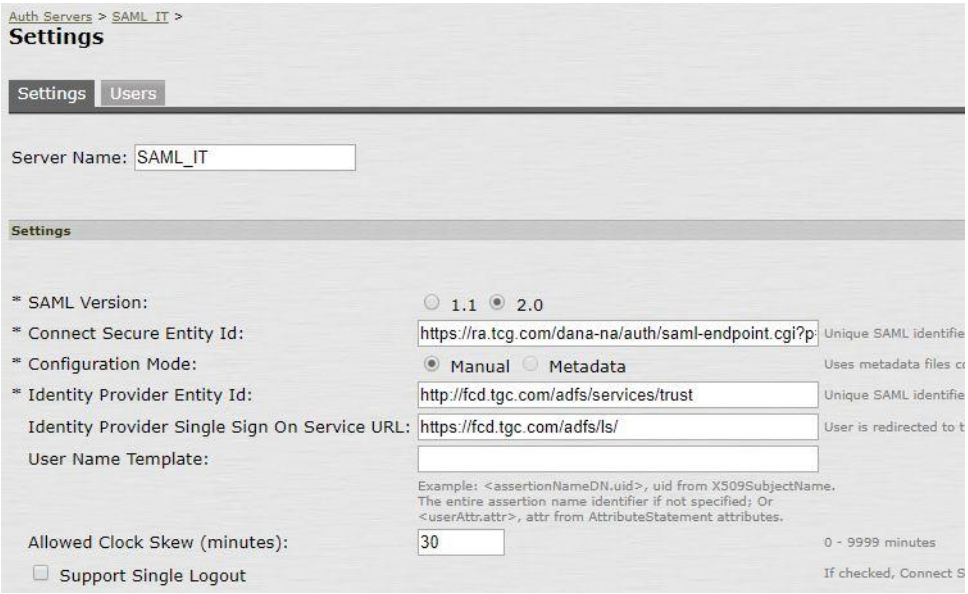

Fig. 4.4.2: Servidor de autenticación de SAML

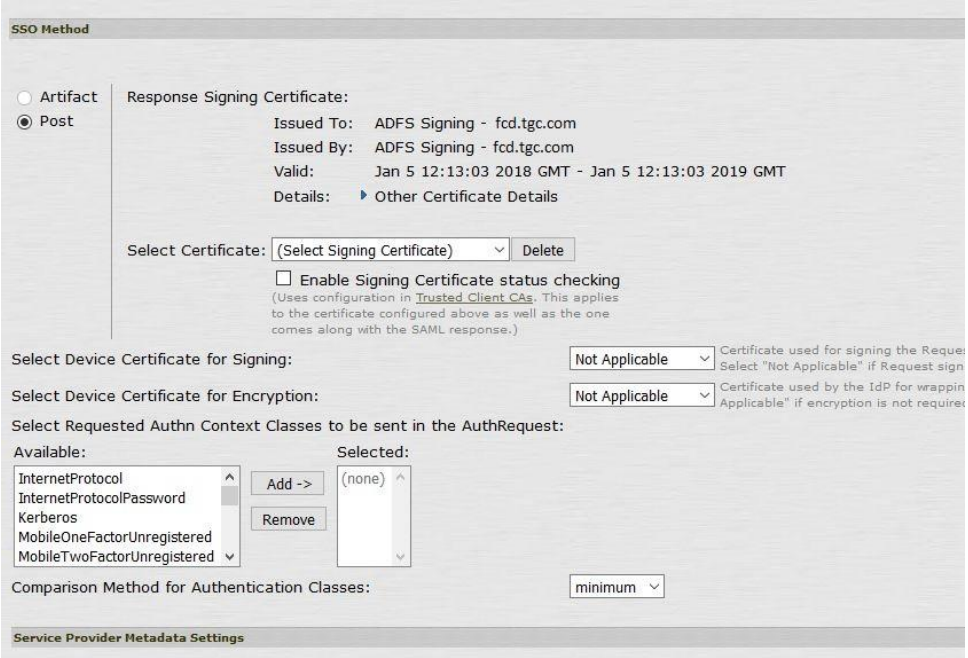

Fig. 4.4.3: Servidor de autenticación de SAML

Con esto queda configurada la autenticación con SAML y el SSO. Ahora cuando un usuario se autentique la primera vez para acceder al agente pesado o a los recursos habilitados para él, pasará un exhaustivo control de seguridad para validar o no sus credenciales. Si se autentica correctamente no tendrá que volver a introducir sus credenciales, pues todas las aplicaciones o accesos tendrán la misma contraseña y ya se ha validado la primera vez contra el SAML.

2. 2FA integrado con TOTP

TOTP (*Time-Based One-Time Password*) [30] [39] [40] es la autenticación con clave de un solo uso basadas en el tiempo. Es decir, es un algoritmo que calcula una contraseña de un solo uso, comúnmente conocido como token, a partir de una clave secreta compartida y la hora actual. La herramienta de Pulse admite la autenticación de TOTP mediante el algoritmo de Google Authenticator para generar la clave secreta compartida y el token, de manera que se pueda usar como opción de autenticación multifactor.

TOTP combina una clave secreta con la marca de tiempo actual utilizando una función de hash criptográfica para generar una contraseña de un solo uso. La marca de tiempo normalmente aumenta en intervalos de 30 segundos, por lo que las contraseñas generadas cercanas en el tiempo desde la misma clave secreta, serán iguales.

En una aplicación típica de autenticación de dos factores, la autenticación de usuario procede de la siguiente manera: un usuario introduce el nombre de usuario y la contraseña en un sitio web u otro servidor, genera una contraseña de un solo uso para el servidor mediante TOTP ejecutado localmente en un dispositivo, y escribe también esa contraseña en el servidor. El servidor entonces ejecuta TOTP para verificar la contraseña de un solo uso introducida. Para que esto funcione, los relojes del dispositivo del usuario y del servidor necesitan estar más o menos

sincronizados. Una sola clave secreta, que se utilizará para todas las sesiones de autenticación posteriores, debe haber sido compartida antes entre el servidor y el dispositivo del usuario por un canal seguro. Si se realizan más pasos, el usuario también puede autenticar el servidor mediante TOTP.

Una vez visto cómo funciona el TOTP, se va a configurar en nuestra herramienta un nuevo servidor de autenticación de tipo TOTP.

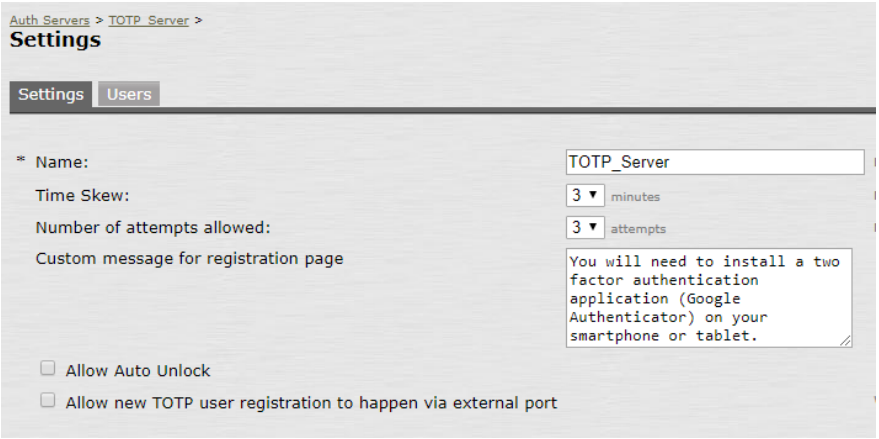

Fig. 4.4.4: Configuración servidor de autenticación TOTP

Una vez finalizado este paso, se deberá crear un nuevo realm en el que se habilitará la opción de un servidor de autenticación adicional al seleccionado, el cual será el TOTP. En este caso se realizará una autenticación de usuarios locales + TOTP.

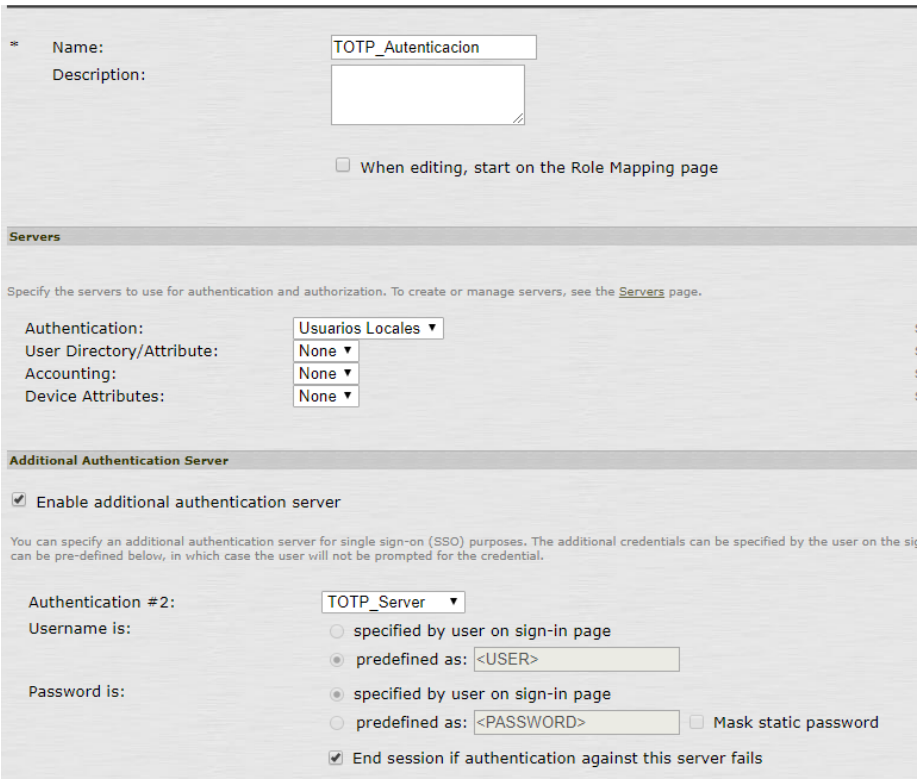

Fig. 4.4.5: Realm con 2FA (usuarios locales + TOTP)

A modo de ejemplo, se va a emular como realizaría un usuario final, perteneciente al realm de usuarios locales, su primer inicio de sesión con TOTP.

Para registrarse por primera vez vía web y tras autenticarse correctamente contra el servidor principal (Usuarios Locales), aparecerá la página para registrarse en TOTP.

Fig. 4.4.6: Registro en TOTP

Tal y como indica los pasos de la figura 4.4.6, se deberá instalar en un móvil/Tablet la aplicación ‘Google Authenticator’ [41] y leer el código QR o introducir un texto proporcionado.

Además, se deberá guardar los códigos posteriores como copia de seguridad en caso de pérdida del dispositivo o error en la conexión con Google Authenticator.

En la siguiente figura se muestra como se realiza la inscripción desde un móvil. Una vez que se ha configurado, la aplicación generará un token cada 30 segundos. [42]

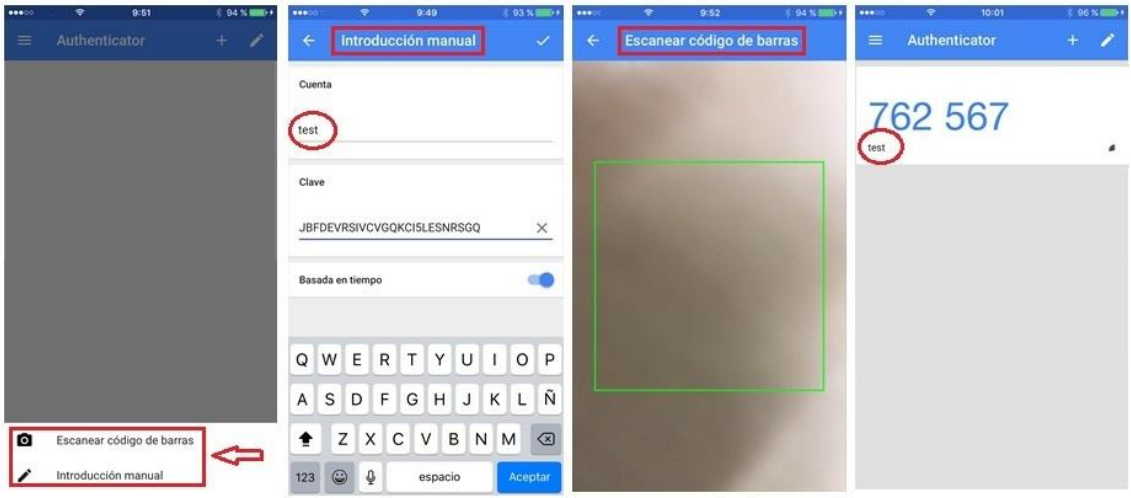

Fig. 4.4.7: Paso a paso para autenticarse en Google Authenticator

Por último, se debe introducir este token en el apartado donde se solicita introducir el token generado en la figura 4.4.6. Si este es correcto, el usuario se autenticará y podrá acceder a su página de inicio donde tiene todos los accesos a sus recursos empresariales.

Para próximos inicios de sesión, este usuario sólo deberá introducir su usuario y contraseña y cuando se valide, le solicitará el token que se ha generado en su móvil. Una vez que este se valide, accederá a su página principal.

5. PRESUPUESTO

En este apartado se va a proponer un presupuesto del proyecto basándose en todos los recursos implicados y necesarios para llevarlo a cabo, así como, la planificación del mismo.

5.1 Planificación del proyecto

El trabajo consistirá en integrar un software, Pulse Secure, en una empresa para facilitar los accesos remotos y mejorar el teletrabajo. Unificándose en una sola herramienta todos los recursos necesarios para que la gestión de las tareas sea lo más amena posible.

Las fases en las que se ha dividido el trabajo son las siguientes:

- Documentación: Búsqueda de información y documentación sobre las herramientas existentes para el acceso remoto, y en concreto, sobre la solución aportada de Pulse Secure. También se ha realizado búsqueda de documentación sobre las necesidades existentes en una empresa, elementos y recursos aplicados.

- Análisis empresarial: Se analizará diferentes empresas para evaluar los recursos que utilizan y las integraciones de las que disponen. Los escenarios que se realizarán se basarán en lo que se obtenga de dicho análisis.

- Obtención de recursos: Obtener el software de Pulse Secure para realizar pruebas, además de una máquina virtual de VMware[4] para poder instalarlo.

- Realización de pruebas: Se creará un entorno de pruebas en una máquina virtual donde se instalará el software de Pulse Secure. Con ello se crearán diferentes escenarios utilizando recursos e integraciones que puede tener una empresa.

ACTIVIDAD	COMIENZO	DURACIÓN DEL PLAN	PERCENT COMPLETE
Búsqueda de información	1	4	100%
Documentarse sobre el software	1	5	100%
Búsqueda documentación integraciones empresariales	1	5	100%
Análisis de la herramienta	4	8	100%
Análisis empresarial	5	6	100%
Instalación del software	8	3	100%
Creación de ambiente para pruebas	10	4	100%
Realizar escenario pruebas	14	6	100%
Elaborar documentación	17	8	100%

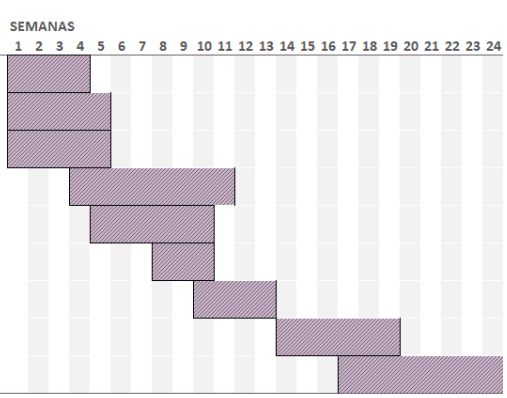

Fig. 5.1.1: Diagrama de Grantt para el trabajo

[4] https://www.vmware.com/es/products/vsphere.html

5.2 Costes

Dentro de los costes intervendrán tanto los costes directos como los indirectos y se realizará un cálculo estipulado de un año y la correspondiente ponderación a los 6 meses de duración del trabajo fin de grado.

Dentro de los costes se tendrán en cuenta la suscripción con Pulse Secure, la necesidad de un ingeniero para instalar y gestionar el servicio ARU, así como los equipos implicados durante todo el proceso.

TABLA 5.2.1
COSTES DE LOS ELEMENTOS UTILIZADOS

Elementos empleados	Precio Licencia al año (€)	Uso correspondiente (meses)	Coste total (€)
SO Windows 10 Home	145,00 €	6	72,5 €
VMware vSphere	639,94 €	6	319,97 €
Licencias Pulse Secure	1.500 €	6	750 €
Office 365	279,00 €	6	139,5 €
Draw.io	free	6	0,00 €

TABLA 5.2.2
COSTES DEL PERSONAL IMPLICADO

	Coste por hora (€)	Horas invertidas (h)	Coste total (€)
Jefe de proyecto	50	220	11.000 €
Técnico	25	260	6.500 €

Teniendo en cuenta que el resto de la infraestructura y de las integraciones forman parte de la empresa, se considerará un gasto asumido. Sólo con el incremento que supone obtener las licencias del software se puede obtener todo lo mostrado anteriormente.

El coste total del proyecto asciende a:

TABLA 5.2.3
COSTES TOTALES DEL PROYECTO

	Coste total (€)
Proyecto	18.781,97 €

6. CONCLUSIONES Y TRABAJOS FUTUROS

6.1 Conclusiones

Una vez finalizada la descripción y uso de la herramienta ARU para integrar diversos recursos empresariales, se ha podido demostrar que esta propuesta se adapta fácilmente a los usos empresariales, sin centrarse en potenciar un recurso, como puede ser el acceso remoto. Esto ofrece a la compañía la oportunidad de obtener, según sus necesidades y configuraciones existentes en su red, una plataforma completa, segura y de fácil manejo.

Como hemos visto a lo largo de este proyecto, se ha dado bastante importancia a la seguridad aplicada a distintos recursos y se han demostrado diferentes maneras de implementación y combinación, como puede ser una integración cuya seguridad aplicada a los usuarios es con un doble factor de autenticación junto con el requisito de host checker aplicado al dispositivo de dicho usuario.

Tras demostrar el uso y realización de integraciones con diferentes niveles de complejidad, se puede afirmar que ARU se adapta a todo tipo de empresas y cuenta con una importante flexibilidad del servicio, pudiendo integrar desde un directorio LDAP a simplemente usuarios locales. Por ello finalmente se puede concluir que se han cumplido los objetivos marcados en este proyecto y que los resultados obtenidos han sido positivos.

6.2 Trabajos futuros

Las necesidades de poder acceder a tus recursos empresariales fuera de la oficina cada vez son más comunes, ya que los trabajadores aprovechan los trayectos de los viajes de trabajo para ir adelantando lo que tienen que realizar en el destino y ultimar los detalles de sus reuniones, o necesitan conectarse de madrugada si ha saltado alguna alarma en los servicios que gestionen las empresas.

Por ello, ya no solo se depende de un ordenador, sino que ahora se disponen de smartphones o tablets en donde pueden realizar ese mismo trabajo. En ocasiones, es más cómodo utilizar el dispositivo móvil y no tener que llevar un ordenador por si se necesita.

Por lo que como trabajo futuro se propone utilizar la misma solución aportada para los ordenadores, pero para los dispositivos móviles y tablets. Es decir, utilizar Pulse Secure aplicado a Smartphones y tablets. Al ser un software compatible con Android, iOS y Windows Phone, el alcance para la implantación de esta solución es muy amplia.

Sería necesario realizar pruebas en diferentes entornos para estudiar su comportamiento, además de comprobar las configuraciones que se ofrecen en cada sistema operativo, pues no tienen por qué soportar las mismas funciones, ya que están basados en sistemas operativos diferentes.

Con ello se podrá mejorar la comunicación usuario $\rightleftarrows$ oficina, consiguiendo mayor comodidad a la hora de tener que realizar ciertas gestiones o accesos a documentación interna, y mejorar la rapidez de acceso pues un Smartphone/Tablet se suele llevar encendido y no necesitas disponer de un sitio para poder trabajar. Con lo cual, se consigue un extra como complemento a la solución aportada para los ordenadores.

Con esta nueva propuesta, se obtendrá un servicio más completo que abarcará todos los sistemas operativos y facilitará el trabajo a los usuarios. Pudiendo conseguir una mejora en la productividad y minimizar los problemas que se puedan ocasionar por no disponer de una herramienta que facilite y gestione los accesos a los diferentes recursos necesarios.

REFERENCIAS Y BIBLIOGRAFÍA

Las referencias se listan por orden de citación en el texto.

Las figuras que aparecen en el documento se han realizado con la herramienta online draw (https://www.draw.io/)

[1] *Information technology -- Service management,* 2015.

[2] *IEEE Standard for Information technology,* 2017.

[3] «General Data Protection Regulation (GDPR),» 2018. [En línea]. Available: https://www.eugdpr.org/eugdpr.org-1.html.

[4] J. R. R. A. A. L.-N. B Desmond, «Active Directory Fundamentals,» de *Active Directory: Designing, Deploying, and Running Active Directory*, O'Reilly Media, Inc, 2008, pp. 17-40.

[5] J. Y. a. R. Campbell, 2007. [En línea]. Available: https://technet.microsoft.com/es-es/library/2007.02.activedirectory.aspx.

[6] G. Keller, «JumpCloud,» 2015. [En línea]. Available: https://jumpcloud.com/blog/difference-between-ldap-and-active-directory/.

[7] J. C. SETH ROSENBLATT, «cnet,» 2015. [En línea]. Available: https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/.

[8] A. J. R. L. R. M. S. a. M. Y. John Brainard, «Fourth-Factor Authentication: Somebody You Know,» 2009. [En línea]. Available: https://www.guanotronic.com/~serge/papers/chi09b.pdf.

[9] DGP, «dnielectronico,» [En línea]. Available: https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_076.

[10] «docs Microsoft,» 2009. [En línea]. Available: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/bb742566(v=technet.10).

[11] C. a. R. A.Yashwanth Reddy, *Performance Evaluation and Design Considerations,* India: Journal of Network Communications and Emerging Technologies (JNCET), 2017.

[12] «thrivenetworks,» 2011. [En línea]. Available: https://www.thrivenetworks.com/blog/pros-and-cons-of-using-a-VPN/.

[13] J. Mason, «The Best VPN,» 2011. [En línea]. Available: https://beebom.com/vpn-pros-cons/.

[14] T. Y. a. C. Lonvick, «ietf,» 2006. [En línea]. Available: https://tools.ietf.org/html/rfc4251.

[15] D. Bider, «ietf,» 2018. [En línea]. Available: https://tools.ietf.org/html/rfc8308.

[16] J. G. J. M. H. F. L. M. P. L. a. T. B.-L. R. Fielding, «ietf,» 1999. [En línea]. Available: https://tools.ietf.org/html/rfc2616.

[17] R. F. a. J. Reschke, «ietf,» 2014. [En línea]. Available: https://tools.ietf.org/html/rfc7230.

[18] A. S., «medium,» 2016. [En línea]. Available: https://medium.com/@alxsanborn/https-ssl-and-ssh-a-conceptual-understanding-9-2-16-4e75ce8d574.

[19] D. Wagner y B. Schneier, «Analysis of the SSL 3.0 protocol,» Counterpane Systems, California, 1997.

[20] K. G. P. a. H. W. Hugo Krawczyk, «On the Security of the TLS Protocol: A Systematic Analysis,» IBM Research, London, 2013.

[21] «hpe,» 2015. [En línea]. Available: http://h22208.www2.hpe.com/eginfolib/networking/docs/switches/5130ei/5200-3946_security_cg/content/485048570.htm.

[22] T. D. a. C. Allen, «rfc-editor,» 1999. [En línea]. Available: https://www.rfc-editor.org/rfc/pdfrfc/rfc2246.txt.pdf.

[23] T. D. a. E. Rescorla, «rfc-editor,» 2008. [En línea]. Available: https://www.rfc-editor.org/rfc/rfc5246.txt.

[24] M. H. J. H. S. S. a. T. v. d. M. Cas Cremers, «A Comprehensive Symbolic Analysis of TLS 1.3,» London, 2017.

[25] S. P. Iglesias, «Análisis del protocolo IPSec: el estándar de seguridad en IP,» España, 2001.

[26] S. K. a. R. Atkinson, «rfc-editor,» 1998. [En línea]. Available: https://www.rfc-editor.org/rfc/rfc2402.txt.

[27] S. Kent, «rfc-editor,» 2005. [En línea]. Available: https://www.rfc-editor.org/rfc/rfc4303.txt.

[28] D. H. a. D. Carrel, «rfc-editor,» 1998. [En línea]. Available: https://www.rfc-editor.org/rfc/rfc2409.txt.

[29] «Pulse Secure,» [En línea]. Available: https://www.pulsesecure.net/connect-secure/overview/.

[30] P. Secure, «Pulse Connect Secure AdministrationGuide,» California, 2017.

[31] P. Secure, «Host Checker,» 2015.

[32] P. Secure, «Endpoint Security Assessment Plugin (ESAP),» 2018.

[33] «Go Daddy,» [En línea]. Available: https://es.godaddy.com/blog/que-es-el-hosting-web-y-para-que-sirve/.

[34] «Office 365,» [En línea]. Available: https://support.office.com/es-es/article/%C2%BFqu%C3%A9-se-incluye-en-office-365-b3bf0f8e-4049-4dd6-b8ab-8ab76d90c06d.

[35] P. Secure, 2017. [En línea]. Available: https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB9536.

[36] «Pulse Secure,» 2017. [En línea]. Available: https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB40426.

[37] P. Secure, 2018. [En línea]. Available: https://www.pulsesecure.net/support/eol/software/pulse-secure-client.

[38] J. H. a. E. Maler, «Security Assertion Markup Language(SAML) V2.0 Technical Overview,» OASIS, 2005.

[39] S. M. M. P. J. R. D. M'Raihi, «rfc-editor,» 2011. [En línea].

[40] C. M. M. Pal, «Cross-site, TOTP-based two factor authentication». Hungary Patente US20170331801, 16 11 2017.

[41] «Google Play,» [En línea]. Available: https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=es.

[42] «Google Support,» [En línea]. Available: https://support.google.com/accounts/answer/1066447?co=GENIE.Platform%3DAndroid&hl=en.